

AUTOMORPHISMS OF LOCAL FIELDS OF PERIOD p AND NILPOTENT CLASS $< p$

VICTOR ABRASHKIN

ABSTRACT. Suppose K is a finite field extension of \mathbb{Q}_p containing a primitive p -th root of unity. Let $\Gamma_K(1)$ be the Galois group of a maximal p -extension of K with the Galois group of period p and nilpotent class $< p$. In the paper we describe the ramification filtration $\{\Gamma_K(1)^{(v)}\}_{v \geq 0}$ and relate it to an explicit form of the Demushkin relation for $\Gamma_K(1)$. The results are given in terms of Lie algebras attached to involved groups by the classical equivalence of the categories of p -groups and Lie algebras of nilpotent class $< p$.

INTRODUCTION

Everywhere in the paper p is a prime number, $p > 2$.

If G is a topological group and $s \in \mathbb{N}$ then $C_s(G)$ is the closure of the subgroup of commutators of order $\geq s$. With this notation, $G/G^p C_s(G)$ is the maximal quotient of G of period p and nilpotent class $< s$. Similarly, if L is a topological Lie \mathbb{F}_p -algebra then $C_s(L)$ is the closure of the ideal of commutators of order $\geq s$ and $L/C_s(L)$ is the maximal quotient of nilpotent class $< s$ of L . For any topological \mathbb{F}_p -module \mathcal{M} we use the notation $L_{\mathcal{M}} = L \hat{\otimes}_{\mathbb{F}_p} \mathcal{M}$.

Suppose $\mathbb{Q}[[X, Y]]$ is a free associative algebra in two variables X and Y with coefficients in \mathbb{Q} . Then the classical Campbell-Hausdorff formula

$$X \circ Y = \log(\exp(X) \cdot \exp(Y)) = X + Y + (1/2)[X, Y] + \dots$$

has p -integral coefficients modulo p -th commutators. Therefore, for any topological Lie \mathbb{F}_p -algebra L of nilpotent class $< p$, we can introduce the topological group $G(L)$ which equals L as a set and is provided with the Campbell-Hausdorff composition law $l_1 \circ l_2 = l_1 + l_2 + (1/2)[l_1, l_2] + \dots$. The correspondence $L \mapsto G(L)$ induces equivalence of the category of Lie \mathbb{F}_p -algebras of nilpotent class $< p$ and the category of p -groups of period p of the same nilpotent class.

Let K be a complete discrete valuation field with finite residue field $k \simeq \mathbb{F}_{p^{N_0}}$, $N_0 \in \mathbb{N}$. Denote by K_{sep} a separable closure of K and set $\text{Gal}(K_{sep}/K) = \Gamma_K$.

Date: October 5, 2015.

Key words and phrases. local field, Galois group, ramification filtration.

A profinite group structure of Γ_K is well-known, [19]. Most significant information about this structure comes from the maximal p -quotient $\Gamma_K(p)$ of Γ_K , [20, 27, 28]. As a matter of fact, the structure of $\Gamma_K(p)$ is not too complicated: its (topological) module of generators equals K^*/K^{*p} and if K has no non-trivial p -th roots of unity (e.g. if $\text{char}K = p$) then $\Gamma_K(p)$ is pro-finite free; otherwise, $\Gamma_K(p)$ has only one (the Demushkin) relation of a very special form.

On the other hand, Γ_K has additional structure given by the decreasing series of normal (ramification) subgroups $\Gamma_K^{(v)}$, $v \geq 0$. This additional structure on Γ_K (or even on the pro- p -group $\Gamma_K(p)$) is sufficient to recover all properties of the original complete discrete valuation field K , [25, 6, 10].

Note that on the level of abelian extensions the ramification filtration of Γ_K^{ab} is completely described by class field theory and has very simple structure. But already on the level of p -extensions with Galois groups of nilpotent class ≥ 2 , the ramification filtration starts demonstrating highly non-trivial behaviour, cf. [2, 4, 16, 17].

In [1, 2, 3] the author introduced new techniques (nilpotent Artin-Schreier theory) which allowed us to work with field extensions of characteristic p with Galois groups of nilpotent class $< p$. As we have mentioned already, such groups come from Lie algebras and our main result describes the ideals coming from ramification subgroups.

Consider the case of complete discrete valuation fields K of mixed characteristic containing a primitive p -th root of unity ζ_1 . Let $K_{<p}$ be the maximal p -extension of K in K_{sep} with the Galois group of nilpotent class $< p$ and period p . Then $\text{Gal}(K_{<p}/K) = \Gamma_K/\Gamma_K^p C_p(\Gamma_K) := \Gamma_K(1)$ is a group with finitely many generators and one relation. (This terminology makes sense in the category of p -groups of nilpotent class $< p$ and period p .) Let $\{\Gamma_K(1)^{(v)}\}_{v \geq 0}$ be the ramification filtration of $\Gamma_K(1)$. If L is a Lie \mathbb{F}_p -algebra such that $\Gamma_K(1) = G(L)$ then for all v , $\Gamma_K(1)^{(v)} = G(L^{(v)})$, where $L^{(v)}$ are ideals in L . In this paper we determine the structure of L and “ramification” ideals $L^{(v)}$. In particular, the Demushkin relation in L appears in our setting in terms related directly to the ramification ideals $L^{(v)}$.

Note that a similar technique (the paper in progress) can be used to treat not only more general groups $\Gamma_K(M) := \Gamma_K/\Gamma_K^{p^M} C_p(\Gamma_K)$, $M \in \mathbb{N}$, but also the case of higher local fields K .

For the first approach to the above problem cf. [32], where the image of the ramification filtration in $C_2(\Gamma_K)/\Gamma_K^p C_3(\Gamma_K)$ was studied under some restrictions to the basic field K . The methods and techniques from [32] could not be applied to a more general situation.

The principal advantage of our method is that from the very beginning we work with the whole group $\Gamma_K(1)$ rather than with the quotients of its central series.

The main steps of our approach can be described as follows.

a) *Relation to the characteristic p case.*

Let π_0 be a fixed uniformizer in K and $\tilde{K} = K(\{\pi_n \mid n \in \mathbb{N}\})$, where $\pi_n^p = \pi_{n-1}$. Then the field-of-norms functor X [30], gives us a complete discrete valuation field $X(\tilde{K}) = \mathcal{K}$ of characteristic p with residue field k and fixed uniformizer t . We have also a natural identification $\Gamma_{\mathcal{K}} = \Gamma_{\tilde{K}}$, which is compatible with the appropriate ramification filtrations in $\Gamma_{\mathcal{K}}$ and Γ_K via the Herbrand function $\varphi_{\tilde{K}/K}$. This gives us the following fundamental short exact sequence in the category of p -groups

$$(0.1) \quad \Gamma_{\mathcal{K}}(1) \xrightarrow{\iota} \Gamma_K(1) \longrightarrow \text{Gal}(K(\pi_1)/K) (= \langle \tau_0 \rangle^{\mathbb{Z}/p}) \longrightarrow 1,$$

where τ_0 is such that $\tau_0(\pi_1) = \zeta_1 \pi_1$.

b) *Nilpotent Artin-Schreier theory.*

This theory allows us to fix an identification $\Gamma_{\mathcal{K}}(1) = G(\mathcal{L})$, where \mathcal{L} is profinite Lie algebra over \mathbb{F}_p . This identification depends only on the above uniformizer t in \mathcal{K} and a choice of $\alpha_0 \in k$ such that $\text{Tr}_{k/\mathbb{F}_p}(\alpha_0) = 1$. Note that this theory also provides us with the system of free generators $\{D_{an} \mid (a, p) = 1, n \in \mathbb{Z}/N_0\} \cup \{D_0\}$ of \mathcal{L}_k .

c) *Ramification filtration in $\Gamma_{\mathcal{K}}(1)$.*

With respect to the above identification $\Gamma_{\mathcal{K}}(1) = G(\mathcal{L})$, the ramification subgroups $\Gamma_{\mathcal{K}}(1)^{(v)}$ come from the ideals $\mathcal{L}^{(v)}$ of \mathcal{L} . In [1, 2, 3] we constructed explicitly the elements $\mathcal{F}_{\gamma, -N}^0 \in \mathcal{L}_k$ with non-negative $\gamma \in \mathbb{Q}$ and $N \in \mathbb{Z}$, such that for any $v \geq 0$ and sufficiently large $N \geq N(v)$, $\mathcal{L}^{(v)}$ appears as the minimal ideal in \mathcal{L} such that $\mathcal{F}_{\gamma, -N}^0 \in \mathcal{L}_k^{(v)}$ for all $\gamma \geq v$.

d) *Fundamental sequence of Lie algebras.*

Using the above mentioned equivalence of the categories of p -groups and Lie algebras we can replace (0.1) by the following exact sequence of Lie \mathbb{F}_p -algebras

$$(0.2) \quad 0 \longrightarrow \mathcal{L}/\mathcal{L}(p) \longrightarrow L \longrightarrow \mathbb{F}_p \tau_0 \longrightarrow 0,$$

where $G(\mathcal{L}(p)) = \text{Ker } \iota$ and $G(L) = \Gamma_K(1)$. If $\tau_{<p}$ is a lift of τ_0 to L then the structure of (0.2) can be given via the differentiation $\text{ad}\tau_{<p}$ on \mathcal{L} .

e) *Replacing τ_0 by $h \in \text{Aut}\mathcal{K}$.*

When studying the structure of (0.2) we can approximate τ_0 by $h \in \text{Aut}\mathcal{K}$. This automorphism h is defined in terms of the expansion of ζ_1 in powers of our fixed uniformizer π_0 . Then the formalism of nilpotent Artin-Schreier theory allows us to specify a lift $\tau_{<p}$, to find the ideal $\mathcal{L}(p)$ and to introduce a recurrent procedure to obtain the values $\text{ad}\tau_{<p}(D_{an}) \in \mathcal{L}_k$ and $\text{ad}\tau_{<p}(D_0) \in \mathcal{L}$.

f) *Structure of L .*

Analyzing the above recurrent procedure modulo $C_2(\mathcal{L}_k)$ we can see that the knowledge of the elements $\text{ad}\tau_{<p}(D_{an})$ allows us to kill all generators D_{an} of \mathcal{L}_k with $a > c_0 := e_K p / (p-1)$. (Here e_K is the ramification index of K over \mathbb{Q}_p .) In other words, L_k has the minimal system of generators $\{D_{an} \mid 1 \leq a < c_0, n \in \mathbb{Z}/N_0\} \cup \{D_0\} \cup \{\tau_{<p}\}$. On the other hand, $\text{ad}\tau_{<p}(D_0) \in C_2(\mathcal{L}_k)$ and, therefore, gives us the (unique) Demushkin relation in L .

g) *Ramification subgroups $L^{(v)}$ in L .*

For $v \geq c_0$, all ramification ideals $L^{(v)} \subset \mathcal{L}/\mathcal{L}(p)$ and come from the appropriate ideals $\mathcal{L}^{(v')}$, where the upper indices v and v' are related by the Herbrand function of the field extension \tilde{K}/K . As one of immediate applications we found for $2 \leq s < p$, the biggest upper ramification numbers of the maximal p -extensions $K[s]$ of K with the Galois groups of period p and nilpotent class $\leq s$. We shall get the remaining ramification ideals $L^{(v)}$ with $v \leq c_0$ if we specify a “good” lift $\tau_{<p}$ of τ_0 , i.e. such that $\tau_{<p} \in L^{(c_0)}$. This is the most difficult part of the paper where we need a technical result from [3].

h) *Explicit formulas for $\text{ad}\hat{\tau}_0$ with “good” $\hat{\tau}_0$.*

The formulas for $\text{ad}\tau_{<p}(D_{an})$ and $\text{ad}\tau_{<p}(D_0)$ can be easily obtained modulo $C_3(L_k)$. In Section 5 we obtain a general formula for $\text{ad}\tau_{<p}(D_0)$. This gives an explicit form of the Demushkin relation in terms of the ramification generators $\mathcal{F}_{\gamma, -N}^0$.

Note that our description of $\Gamma_K(1)$ together with its ramification filtration may serve as a guide to what we could expect a nilpotent local class field theory should be. Our approach gives the objects of this theory on the level of quotients of nilpotent class $< p$ together with induced ramification filtration. Regretfully, our description is not functorial: it depends on a choice of uniformizing element in K .

It would be very interesting to compare our results with the construction of Γ_K in [23], cf. also [21]. This construction uses iterations of the Lubin-Tate theories via the field-of-norms functor and is done inside the group of formal power series with the operation given by their composition. At the moment, it is not clear how to extract from this construction even well-known properties of, say, the pro- p -group $\Gamma_K(p)$.

The content of this paper is arranged in a slightly different order compared to above principal steps a)-h). In Section 1 we briefly discuss auxiliary facts and constructions from the characteristic p case. In Section 2 we study an analogue \mathcal{G}_h of $\Gamma_K(1)$ which appears if we replace τ_0 by a suitable $h \in \text{Aut}\mathcal{K}$; we also describe the commutator subgroups of \mathcal{G}_h and, in particular, find the ideal $\mathcal{L}(p) = C_p(\mathcal{G}_h)$. In Section 3 we develop the techniques allowing us to switch the languages of p -groups and Lie algebras. In Section 4 we establish the Criterion to characterize

“good” lifts $h_{<p}$ of h and in Section 5 we compute $\text{adh}_{<p}(D_0)$ for such “good” lifts. Finally, in Section 6 we prove that all our results obtained for the group \mathcal{G}_h are actually valid for the group $\Gamma_K(1)$.

Notation. In the main body of the paper we use slightly different notation: $\Gamma_K(1)$ is denoted by $\Gamma_{<p}$, Γ_K — by \mathcal{G} and $\Gamma_K(1)$ — by $\mathcal{G}_{<p}$.

1. PRELIMINARIES

1.1. Covariant nilpotent Artin-Schreier theory. Suppose \mathcal{K} is a field of characteristic p , \mathcal{K}_{sep} is a separable closure of \mathcal{K} and $\mathcal{G} = \text{Gal}(\mathcal{K}_{sep}/\mathcal{K})$. We assume that the composition $g_1 g_2$ of $g_1, g_2 \in \mathcal{G}$ is such that for any $a \in \mathcal{K}_{sep}$, $g_1(g_2 a) = (g_1 g_2)a$.

In [1, 2, 3] we developed a nilpotent analogue of the classical Artin-Schreier theory of cyclic extensions of fields of characteristic p . The main results of this theory (which will be called the contravariant nilpotent Artin-Schreier theory) can be briefly explained as follows.

Let \mathcal{G}^0 be the group such that $\mathcal{G}^0 = \mathcal{G}$ as sets but for any $g_1, g_2 \in \mathcal{G}$ their composition in \mathcal{G}^0 equals $g_2 g_1$. In other words, we assume that \mathcal{G}^0 acts on \mathcal{K}_{sep} via $(g_1 g_2)a = g_2(g_1(a))$.

Let L be a Lie \mathbb{F}_p -algebra of nilpotent class $< p$. Then the absolute Frobenius σ and \mathcal{G} act on $L_{\mathcal{K}_{sep}}$ through the second factor. We have $L_{\mathcal{K}_{sep}}|_{\sigma=\text{id}} = L$ and $(L_{\mathcal{K}_{sep}})^{\mathcal{G}} = L_{\mathcal{K}}$.

For any $e \in G(L_{\mathcal{K}})$, the set of $f \in G(L_{\mathcal{K}_{sep}})$ such that $\sigma(f) = f \circ e$ is not empty. Define the group homomorphism $\pi_f^0(e) : \mathcal{G}^0 \rightarrow G(L)$ by setting for $g \in \mathcal{G}$, $\pi_f^0(e) : g \mapsto g(f) \circ (-f)$.

Remark. Strictly speaking $g(f)$, where $g \in \mathcal{G}$, should be written in the form $(\text{id}_{\mathcal{L}} \otimes g)f$ but in most cases we shall use the first notation. On the other hand, we would prefer the second notation if, say, $g \in \text{Aut} \mathcal{K}_{sep}$ and $g|_{\mathcal{K}} \neq \text{id}_{\mathcal{K}}$. Similarly, we agree to use the notation σ instead of $\text{id}_{\mathcal{L}} \otimes \sigma$.

We have the following properties:

- a) for any group homomorphism $\eta : \mathcal{G}^0 \rightarrow G(L)$ there are $e_{\eta} \in G(L_{\mathcal{K}})$ and $f_{\eta} \in G(L_{\mathcal{K}_{sep}})$ such that $\sigma(f_{\eta}) = f_{\eta} \circ e_{\eta}$ and $\eta = \pi_{f_{\eta}}^0(e_{\eta})$;
- b) two homomorphisms $\pi_f^0(e)$ and $\pi_{f_1}^0(e_1)$ from \mathcal{G}^0 to $G(L)$ are conjugated via some element from $G(L)$ iff there is an $x \in G(L_{\mathcal{K}})$ such that $e_1 = (-x) \circ e \circ \sigma(x)$.

The covariant version of the above theory can be developed quite similarly. We just use the relations $\sigma(f) = e \circ f$ and $g \mapsto (-f) \circ g(f)$ to define the group homomorphism $\pi_f(e) : \mathcal{G} \rightarrow G(L)$. Then we have the obvious analogs of above properties a) and b) with the opposite formula $e_1 = \sigma(x) \circ e \circ (-x)$ for e_1 .

In this paper we use the covariant theory but need some results from [3] which were obtained in the contravariant setting. These results can

be adjusted to the covariant theory just by replacing all involved group or Lie structures to the opposite ones, e.g. cf. Subsection 1.4 below.

1.2. Lifts of analytic automorphisms. Let $\text{Aut}\mathcal{K}$ and $\text{Aut}\mathcal{K}_{sep}$ be the groups of continuous automorphisms of \mathcal{K} and \mathcal{K}_{sep} , respectively. For $h \in \text{Aut}\mathcal{K}$, let $h_{sep} \in \text{Aut}\mathcal{K}_{sep}$ be such that $h_{sep}|_{\mathcal{K}} = h$.

Suppose L is a Lie \mathbb{F}_p -algebra of nilpotent class $< p$. Let $e \in G(L_{\mathcal{K}})$ and choose $f \in G(L_{\mathcal{K}_{sep}})$ such that $\sigma(f) = e \circ f$, set $\eta = \pi_f(e)$ and $\mathcal{K}_e = \mathcal{K}_{sep}^{\text{Ker}\eta}$. Then \mathcal{K}_e does not depend on a choice of f : if $f' \in G(L_{\mathcal{K}_{sep}})$ is such that $\sigma(f') = e \circ f'$ then $f' = f \circ l$ with $l \in G(L)$ and $\text{Ker}\eta = \text{Ker}\pi_{f'}(e)$.

Proposition 1.1. *Suppose $\eta : \mathcal{G} \longrightarrow G(L)$ is epimorphic. Then the following conditions are equivalent:*

- a) $h_{sep}(\mathcal{K}_e) = \mathcal{K}_e$;
- b) *there are $c \in G(L_{\mathcal{K}})$ and $A \in \text{Aut}L$ such that $(\text{id}_{\mathcal{L}} \otimes h_{sep})(f) = c \circ (A \otimes \text{id}_{\mathcal{K}_{sep}})(f)$.*

Proof. Let $e_1 = (\text{id}_L \otimes h)(e)$, $f_1 = (\text{id}_L \otimes h_{sep})(f)$ and $\eta_1 = \pi_{f_1}(e_1)$. Then for any $g \in \mathcal{G}$, we have $\eta_1(g) = (-f_1) \circ g(f_1) =$

$$(\text{id}_L \otimes h)((-f) \circ (h_{sep}^{-1} g h_{sep})(f)) = \eta(h_{sep}^{-1} g h_{sep}).$$

Therefore, η_1 is equal to the composition of the conjugation by h_{sep} (we shall denote it by $\text{Ad}h_{sep}$ below) and η . Then $h_{sep}(\mathcal{K}_e) = \mathcal{K}_e$ means that $\text{Ker}\eta = \text{Ker}\eta_1$. This implies the existence of an automorphism A of the group $G(L)$ (which is automatically automorphism of the Lie algebra L) such that $\eta_1 = A\eta$.

Now let $f' = (A \otimes \text{id}_{\mathcal{K}_{sep}})(f)$ and $e' = (A \otimes \text{id}_{\mathcal{K}})e$. Then $\pi_{f'}(e')(g) = (A \otimes \text{id}_{\mathcal{K}_{sep}})((-f) \circ g(f)) = (A\eta)(g) = \eta_1(g)$. This means that f' and f_1 give the same morphisms $\mathcal{G} \rightarrow G(L)$ and there is an $c \in G(L_{\mathcal{K}})$ such that $f_1 = c \circ f'$, that is a) implies b). Proceeding in the opposite direction we deduce b) from a). \square

1.3. The identification η_0 . Let $\mathcal{K} = k((t))$ be a complete discrete valuation field of Laurent formal power series in variable t with coefficients in $k \simeq \mathbb{F}_{p^{N_0}}$, $N_0 \in \mathbb{N}$. Choose $\alpha_0 \in k$ such that $\text{Tr}_{k/\mathbb{F}_p}\alpha_0 = 1$.

Let $\mathbb{Z}^+(p) = \{a \in \mathbb{N} \mid (a, p) = 1\}$ and $\mathbb{Z}^0(p) = \mathbb{Z}^+(p) \cup \{0\}$. Denote by $\tilde{\mathcal{L}}_k$ a free pro-finite Lie algebra over k with the set of free generators $\{D_{an} \mid a \in \mathbb{Z}^+(p), n \in \mathbb{Z}/N_0\} \cup \{D_0\}$. Denote by the same symbol σ , the σ -linear automorphism of $\tilde{\mathcal{L}}_k$ such that $\sigma : D_0 \mapsto D_0$ and for all $a \in \mathbb{Z}^+(p)$ and $n \in \mathbb{Z}/N_0$, $\sigma : D_{an} \mapsto D_{a, n+1}$. Then $\tilde{\mathcal{L}}^0 := \tilde{\mathcal{L}}_k|_{\sigma=\text{id}}$ is a free pro-finite Lie \mathbb{F}_p -algebra and $\tilde{\mathcal{L}}_k = \tilde{\mathcal{L}}^0_k$.

Let $\mathcal{L} = \tilde{\mathcal{L}}^0/C_p(\tilde{\mathcal{L}}^0)$.

For any $n \in \mathbb{Z}/N_0$, set $D_{0n} = \sigma^n(\alpha_0)D_0$.

Let $e = \sum_{a \in \mathbb{Z}^0(p)} t^{-a} D_{a0} \in G(\mathcal{L}_K)$ and let $f \in G(\mathcal{L}_{K_{sep}})$ be such that $\sigma(f) = e \circ f$.

Then the morphism $\pi_f(e)$ induces the isomorphism of topological groups $\eta_0 : \mathcal{G}_{< p} := \mathcal{G}/\mathcal{G}^p C_p(\mathcal{G}) \xrightarrow{\sim} G(\mathcal{L})$.

In the remaining part of the paper we shall use (without additional notice) the above introduced notation e , f and η_0 . We shall also use the notation $\mathcal{K}_{< p} := \mathcal{K}_{sep}^{\mathcal{G}^p C_p(\mathcal{G})}$.

Note that $f \in G(\mathcal{L}_{K_{< p}})$. In particular, if $h_1, h_2 \in \text{Aut } \mathcal{K}_{sep}$ are such that $(\text{id} \otimes h_1)f = (\text{id} \otimes h_2)f$ then $h_1|_{\mathcal{K}_{< p}} = h_2|_{\mathcal{K}_{< p}}$. Therefore, the appropriate choice of $c \in \mathcal{L}_K$ and $A \in \text{Aut } \mathcal{L}$ from Proposition 1.1 describes efficiently all lifts of automorphisms of \mathcal{K} to automorphisms of $\mathcal{K}_{< p}$. We shall also use below in Subsection 4.4 the following interpretation of this property. Suppose $\mathcal{L}' \subset \mathcal{L}$ is a Lie subalgebra and $\mathcal{K}_{< p}^{G(\mathcal{L}')} = \mathcal{K}'$. Then $f \bmod \mathcal{L}'_{\mathcal{K}_{< p}}$ is defined over \mathcal{K}' . In other words, $f \bmod \mathcal{L}'_{\mathcal{K}_{< p}} \in (\mathcal{L}/\mathcal{L}')_{\mathcal{K}'}$, or $f \in \mathcal{L}_{\mathcal{K}'} + \mathcal{L}'_{\mathcal{K}_{< p}}$.

If $h \in \text{Aut } \mathcal{K}$ then its lift to $\text{Aut } \mathcal{K}_{< p}$ will be denoted usually by $h_{< p}$. The formalism of nilpotent Artin-Shreier theory will allow us to specify the choice of such lifts, cf. Proposition 1.1b).

1.4. The ramification subgroups in $\mathcal{G}_{< p}$. For $v \geq 0$, let $\mathcal{G}_{< p}^{(v)}$ be the image of the ramification subgroup $\mathcal{G}^{(v)}$ of \mathcal{G} in $\mathcal{G}_{< p}$. This subgroup corresponds to some ideal $\mathcal{L}^{(v)}$ of the Lie algebra \mathcal{L} with respect to the identification η_0 .

For $\gamma \geq 0$ and $N \in \mathbb{N}$, introduce $\mathcal{F}_{\gamma, -N}^0 \in \mathcal{L}_k$ such that

$$\mathcal{F}_{\gamma, -N}^0 = \sum_{\substack{1 \leq s \leq p \\ a_i, n_i}} a_1 \eta(n_1, \dots, n_s) [\dots [D_{a_1 \bar{n}_1}, D_{a_2 \bar{n}_2}], \dots, D_{a_s \bar{n}_s}]$$

Here:

— all $a_i \in \mathbb{Z}^0(p)$, $n_i \in \mathbb{Z}$, $0 = n_1 \geq n_2 \geq \dots \geq n_s \geq -N$, $\bar{n}_i = n_i \bmod N_0$;

— $a_1 p^{n_1} + a_2 p^{n_2} + \dots + a_s p^{n_s} = \gamma$;

— if $0 = n_1 = \dots = n_{s_1} > \dots > n_{s_{r-1}+1} = \dots = n_{s_r}$ then $\eta(n_1, \dots, n_s) = (s_1! \dots (s_r - s_{r-1})!)^{-1}$; otherwise, $\eta(n_1, \dots, n_s) = 0$.

Theorem 1.2. *For any $v \geq 0$, there is $\tilde{N}(v)$ such that if $N \geq \tilde{N}(v)$ is fixed then the ideal $\mathcal{L}^{(v)}$ is the minimal ideal in \mathcal{L} such that its extension of scalars $\mathcal{L}_k^{(v)}$ contains all $\mathcal{F}_{\gamma, -N}^0$ with $\gamma \geq v$.*

The appropriate theorem in the contravariant setting was obtained in [3] and uses the elements $\mathcal{F}_{\gamma, -N}$ given by the same formula but with the factor $(-1)^{s-1}$. Indeed, when switching to the covariant setting all commutators of the form $[\dots [D_1, D_2], \dots, D_s]$ should be replaced by $[D_s, \dots, [D_2, D_1] \dots] = (-1)^{s-1} [\dots [D_1, D_2], \dots, D_s]$.

2. THE GROUPS $\tilde{\mathcal{G}}_h$ AND \mathcal{G}_h

2.1. The automorphism h . Let $c_0 \in p\mathbb{N}$. Denote by h a continuous automorphism of \mathcal{K} such that $h|_k = \text{id}$ and

$$h(t) = t \left(1 + \sum_{i \geq 0} \alpha_i(h) t^{c_0 + pi} \right)$$

where all $\alpha_i(h) \in k$ and $\alpha_0(h) \neq 0$. This automorphism will be fixed in the remaining part of the paper.

Let $\widetilde{\exp}(X) = \sum_{0 \leq i < p} X^i / i!$ be the truncated exponential.

Proposition 2.1.

- a) There is $\varepsilon \in t^{c_0/p} O_{\mathcal{K}}^*$ such that $h(t) = t \widetilde{\exp}(\varepsilon^p) \bmod t^{1+pc_0}$;
- b) For any $n \geq 0$, $h^n(t) \equiv t \widetilde{\exp}(n\varepsilon^p) \bmod t^{1+pc_0}$.

Proof. The first statement is obvious. For the second statement note that $h(t) \equiv t \bmod t^{c_0}$ implies that $h(t^{c_0+pi}) \equiv t^{c_0+pi} \bmod t^{pc_0}$ and, therefore, $h(\varepsilon^p) \equiv \varepsilon^p \bmod t^{pc_0}$. It remains to apply induction on n . \square

2.2. Specification of $h_{<p}$. It will be convenient below to specify a lift $h_{<p}$ of h to $\mathcal{K}_{<p}$ using the formalism of nilpotent Artin-Schreier theory as follows.

Define the continuous \mathbb{F}_p -linear operators $\mathcal{R}, \mathcal{S} : \mathcal{L}_{\mathcal{K}} \longrightarrow \mathcal{L}_{\mathcal{K}}$ as follows.

Suppose $\alpha \in \mathcal{L}_k$.

If $n > 0$ then set $\mathcal{R}(t^n \alpha) = 0$ and $\mathcal{S}(t^n \alpha) = -\sum_{i \geq 0} \sigma^i(t^n \alpha)$.

For $n = 0$, set $\mathcal{R}(\alpha) = \alpha_0 \text{Tr}_{k/\mathbb{F}_p} \alpha$, $\mathcal{S}(\alpha) = \sum_{0 \leq j < i < N_0} \sigma^j \alpha_0 \sigma^i \alpha$.

If $n = -n_1 p^m$ with $\gcd(n_1, p) = 1$ then set $\mathcal{R}(t^n \alpha) = t^{-n_1} \sigma^{-m} \alpha$ and $\mathcal{S}(t^n \alpha) = \sum_{1 \leq i \leq m} \sigma^{-i}(t^n \alpha)$.

The proof of the following lemma is straightforward.

Lemma 2.2. For any $b \in \mathcal{L}_{\mathcal{K}}$,

- a) $b = \mathcal{R}(b) + (\sigma - \text{id}_{\mathcal{L}_{\mathcal{K}}})(\mathcal{S}(b))$;
- b) $\mathcal{R}(b) \in \sum_{a \in \mathbb{Z}^+(p)} t^{-a} \mathcal{L}_k + \alpha_0 \mathcal{L}$;

Remark. The definition of the above operators \mathcal{R} and \mathcal{S} in the cases $n > 0$ and $n < 0$ is self-explanatory. In the case $n = 0$ we have the following picture behind. For $\alpha \in \mathcal{L}_k$ and $0 \leq i < N_0$, set $\mathcal{R}_i(\alpha) = \alpha_0 \sigma^{-i} \alpha$ and $\mathcal{S}_i(\alpha) = \sum_{0 \leq j < i} \sigma^j(\mathcal{R}_i(\alpha))$. Then

$$\begin{aligned} \alpha &= \sum_{0 \leq i < N_0} (\sigma^i \alpha_0) \alpha = \sum_{0 \leq i < N_0} \sigma^i \mathcal{R}_i(\alpha) = \sum_{0 \leq i < N_0} ((\sigma - \text{id}) \mathcal{S}_i + \mathcal{R}_i)(\alpha) \\ \mathcal{R} &= \sum_{0 \leq i < N_0} \mathcal{R}_i, \quad \mathcal{S} = \sum_{0 \leq i < N_0} \mathcal{S}_i, \\ \mathcal{S}(\alpha) &= \sum_{0 \leq j < i < N_0} \sigma^j(\alpha_0 \sigma^{-i} \alpha) = \sum_{0 \leq j < i_1 < N_0} \sigma^j \alpha_0 \sigma^{i_1} \alpha, \end{aligned}$$

where $i_1 = j - i + N_0$. Note that there are many other ways to define \mathcal{S} in the case $n = 0$.

For any lift $h_{<p}$, we have $(\text{id}_{\mathcal{L}} \otimes h_{<p})(f) = c \circ (A \otimes \text{id}_{\mathcal{K}_{<p}})(f)$, where $c \in \mathcal{L}_{\mathcal{K}}$ and $A = \text{Ad}(h_{<p}) \in \text{Aut } \mathcal{L}$ can be found from the relation

$$(2.1) \quad (\text{id}_{\mathcal{L}} \otimes h)(e) \circ c = (\sigma c) \circ (A \otimes \text{id}_{\mathcal{K}})(e),$$

cf. Subsection 1.2. This allows us to specify $h_{<p}$ step by step proceeding from $(\text{id}_{\mathcal{L}} \otimes h_{<p})f \bmod C_s(\mathcal{L}_{\mathcal{K}_{<p}})$ to $(\text{id}_{\mathcal{L}} \otimes h_{<p})f \bmod C_{s+1}(\mathcal{L}_{\mathcal{K}_{<p}})$ where $1 \leq s < p$.

Indeed, suppose c and A have been already chosen modulo s -th commutators. Then $c = c'_s + X_s$ and $A = A'_s + A_s$, where $\deg c'_s < s$, $\deg X_s \geq s$ and for any $a \in \mathbb{Z}^0(p)$, $\deg A'_s(D_{a0}) < s$ and $\deg A_s(D_{a0}) \geq s$. (The degrees come from the Lie algebra $\tilde{\mathcal{L}}$ uniquely determined by setting $\deg(D_{a0}) = 1$ for all $a \in \mathbb{Z}^0(p)$.) Then (2.1) implies that

$$(2.2) \quad \sigma X_s - X_s + \sum_{a \in \mathbb{Z}^0(p)} t^{-a} A_s(D_{a0}) \equiv$$

$$(\text{id}_{\mathcal{L}} \otimes h)e \circ c'_s - \sigma c'_s \circ (A'_s \otimes \text{id}_{\mathcal{K}})e \bmod C_{s+1}(\mathcal{L}_{\mathcal{K}}).$$

At the s -th step recurrence relation (2.2) uniquely determines the elements $A_s(D_{a0}) \bmod C_{s+1}(\mathcal{L}_k)$ but the element X_s is determined only up to elements of $C_s(\mathcal{L}) \bmod C_{s+1}(\mathcal{L})$. (This will affect the right-hand side of (2.3) at the next $(s+1)$ -th step and so on.) At the same time the number of different extensions of a given automorphism of $\mathcal{K}_{<p}^{C_s(\mathcal{L})}$ to an automorphism of $\mathcal{K}_{<p}^{C_{s+1}(\mathcal{L})}$ equals

$$[\mathcal{K}_{<p}^{C_{s+1}(\mathcal{L})} : \mathcal{K}_{<p}^{C_s(\mathcal{L})}] = [C_s(\mathcal{L}) : C_{s+1}(\mathcal{L})].$$

Therefore, this recurrent procedure provides us with all lifts $h_{<p}$ of h . In particular, some element $(\text{id}_{\mathcal{L}} \otimes h_{<p})f$ can be uniquely specified if we take at each s -th step the solutions of (2.2) modulo $(s+1)$ -th commutators in the form $\sum_{a \in \mathbb{Z}^0(p)} t^{-a} A_s(D_{a0}) = \mathcal{R}(B_s)$ and $X_s = \mathcal{S}(B_s)$, where B_s is the RHS in (2.2).

Note that it is not easy to control a choice of lifts $h_{<p}$ because the right-hand side of (2.2) contains highly non-trivial Campbell-Hausdorff operation \circ . In Subsection 3 we resolve this problem by using the procedure of linearization.

Remark. If we start with the identity automorphism $\text{id}_{\mathcal{K}}$ instead of h then its lifts to $\mathcal{K}_{<p}$ will be (according to Subsection 1.1) just $\eta_0^{-1}(l^0) \in \mathcal{G}_{<p}$, where $l^0 \in \mathcal{L}$. The appropriate action on f appears in the form $(\text{id}_{\mathcal{L}} \otimes \eta_0^{-1}(l^0))f = f \circ l^0$. On the other hand, the above formalism should describe it in the form $f \mapsto c \circ (A \otimes \text{id}_{\mathcal{K}_{<p}})f$, with $c \in \mathcal{L}_{\mathcal{K}}$ and $A \in \text{Aut } \mathcal{L}$. Verify that $c = l^0$ and $A = \text{Ad } l^0$. Indeed, if $f = \sum_{l \in \mathcal{L}} f_l l$, where all $f_l \in \mathcal{K}_{<p}$ then $f \circ l^0 = l^0 \circ (\sum_{l \in \mathcal{L}} f_l (-l^0) \circ l \circ l^0)$.

2.3. The group $\tilde{\mathcal{G}}_h$. Denote by $\tilde{\mathcal{G}}_h$ the group of all lifts $\tilde{h}_{<p} \in \text{Aut } \mathcal{K}_{<p}$ of the elements \tilde{h} of the closed subgroup in $\text{Aut } \mathcal{K}$ generated by h .

Use the identification η_0 from Subsection 1.3 to obtain a natural short exact sequence of profinite p -groups

$$(2.3) \quad 1 \longrightarrow G(\mathcal{L}) \longrightarrow \tilde{\mathcal{G}}_h \longrightarrow \langle h \rangle \longrightarrow 1$$

For any $s \geq 2$, $C_s(\tilde{\mathcal{G}}_h)$ is a subgroup in $G(\mathcal{L})$ and, therefore, $C_s(\tilde{\mathcal{G}}_h) := \mathcal{L}_h(s)$ is a Lie subalgebra of \mathcal{L} . Set $\mathcal{L}_h(1) = \mathcal{L}$. Note that for any $s_1, s_2 \geq 1$, we have $[\mathcal{L}_h(s_1), \mathcal{L}_h(s_2)] \subset \mathcal{L}_h(s_1 + s_2)$.

Define the weight filtration $\mathcal{L}(s)$, $s \in \mathbb{N}$, in \mathcal{L} by setting $\text{wt}(D_{an}) = s$ if $(s-1)c_0 \leq a < sc_0$. With this notation $\mathcal{L}(s)_k$ is generated over k by all $[\dots [D_{a_1 n_1}, D_{a_2 n_2}], \dots, D_{a_r n_r}]$ such that $\sum_i \text{wt}(D_{a_i n_i}) \geq s$. For any $s_1, s_2 \geq 1$, we also have that $[\mathcal{L}(s_1), \mathcal{L}(s_2)] \subset \mathcal{L}(s_1 + s_2)$.

Theorem 2.3. *For all $s \in \mathbb{N}$, $\mathcal{L}_h(s) = \mathcal{L}(s)$.*

Proof. Let $\mathcal{L}^{lin} = \left(\sum_{a,n} k D_{an} \right)_{\sigma=\text{id}}$ be “the subspace of linear terms” of \mathcal{L} . We have the following properties:

- $\mathcal{L}(s+1) = \mathcal{L}^{lin} \cap \mathcal{L}(s+1) + \mathcal{L}(s+1) \cap C_2(\mathcal{L})$;
- $\mathcal{L}(s+1) \cap C_2(\mathcal{L}) = \sum_{s_1+s_2=s+1} [\mathcal{L}(s_1), \mathcal{L}(s_2)]$;
- $\mathcal{L}_h(s+1)$ is the ideal in \mathcal{L} generated by $[\mathcal{L}_h(s), \mathcal{L}]$ and the elements of the form $(\text{Ad} h_{<p})l \circ (-l)$, where $l \in \mathcal{L}_h(s)$.

Let $(\text{Ad} h_{<p})D_0 = \tilde{D}_0$ and for all $a \in \mathbb{Z}^+(p)$, $(\text{Ad} h_{<p})D_{a0} = \tilde{D}_{a0}$.

Lemma 2.4. *We have:*

- a) $\tilde{D}_0 \equiv D_0 \pmod{(\mathcal{L}(3) + \mathcal{L}(2) \cap C_2(\mathcal{L}))}$;
- b) if $a \in \mathbb{Z}^+(p)$ and $\text{wt}(D_{an}) = s$ then

$$\tilde{D}_{a0} \equiv D_{a0} - \sum_{i \geq 0} \alpha_i(h) a D_{a+c_0+pi,0} \pmod{(\mathcal{L}(s+2)_k + \mathcal{L}(s+1)_k \cap C_2(\mathcal{L}_k))},$$

where $\alpha_i(h) \in k$ are such that $h(t) = t(1 + \sum_{i \geq 0} \alpha_i(h)t^{c_0+pi})$.

We prove this Lemma below after finishing the proof of Theorem 2.3. Clearly, Lemma 2.4 has the following corollaries:

- (c1) if $l \in \mathcal{L}(s)$ then $(\text{Ad} h_{<p})l \circ (-l) \in \mathcal{L}(s+1)$;
- (c2) if $l \in \mathcal{L}^{lin} \cap \mathcal{L}(s+1)$ then there is an $l' \in \mathcal{L}^{lin} \cap \mathcal{L}(s)$ such that $\text{Ad} h_{<p}(l') \circ (-l') \equiv l \pmod{\mathcal{L}(s+1) \cap C_2(\mathcal{L})}$ (use that $\alpha_0(h) \neq 0$).

Prove theorem by induction on $s \geq 1$.

Clearly, $\mathcal{L}_h(1) = \mathcal{L}(1)$.

Suppose $s_0 \geq 1$ and for $1 \leq s \leq s_0$, $\mathcal{L}_h(s) = \mathcal{L}(s)$.

Then $[\mathcal{L}_h(s_0), \mathcal{L}] = [\mathcal{L}(s_0), \mathcal{L}(1)] \subset \mathcal{L}(s_0+1)$ and applying (c1) we obtain that $\mathcal{L}_h(s_0+1) \subset \mathcal{L}(s_0+1)$.

In the opposite direction, note that by inductive assumption,

$$\mathcal{L}(s_0 + 1) \cap C_2(\mathcal{L}) = \sum_{s_1 + s_2 = s_0 + 1} [\mathcal{L}_h(s_1), \mathcal{L}_h(s_2)] \subset \mathcal{L}_h(s_0 + 1)$$

and then from (c2) we obtain that $\mathcal{L}^{lin} \cap \mathcal{L}(s_0 + 1) \subset \mathcal{L}_h(s_0 + 1)$. So, $\mathcal{L}(s_0 + 1) \subset \mathcal{L}_h(s_0 + 1)$ and Theorem 2.3 is completely proved. \square

Proof of Lemma 2.4. Let

$$\mathcal{N} = \sum_{s \geq 1} t^{-c_0 s} \mathcal{L}(s)_m,$$

where m is the maximal ideal of the valuation ring O_K of K . Clearly, \mathcal{N} has a structure of Lie algebra over \mathbb{F}_p and $e \in \mathcal{N}$.

For any $i \geq 0$, introduce the ideals $\mathcal{N}(i) := t^{c_0 i} \mathcal{N}$ of \mathcal{N} . Note that for all $i \geq 0$, the operators \mathcal{R} and \mathcal{S} map $\mathcal{N}(i)$ to itself.

Let

$$\tilde{e} := (\text{Ad} h_{<p} \otimes \text{id})e = \sum_{a \in \mathbb{Z}^0(p)} t^{-a} \tilde{D}_{a0} + \alpha_0 \tilde{D}_0.$$

Then \tilde{e} can be recovered from the relation

$$(2.4) \quad (\text{id}_{\mathcal{L}} \otimes h)e \circ c = (\sigma c) \circ \tilde{e},$$

where $c \in G(\mathcal{L}_K)$, cf. Subsection 2.2.

Note that $e \in \mathcal{N}$ and, therefore, $c, \sigma c \in \mathcal{N}$. (Use that \mathcal{R} and \mathcal{S} map \mathcal{N} to itself.)

Use (2.4) to obtain the following properties of \tilde{e} :

- $(\text{id} \otimes h)e = e + e_1 \bmod \mathcal{N}(2)$, where $e_1 \in \mathcal{N}(1)$ and is equal modulo $\mathcal{N}(2)$ to

$$- \sum_{i \geq 0} \left(\sum_{a \in \mathbb{Z}^+(p)} t^{-a} a \alpha_i(h) D_{a+c_0+pi,0} + \sum_{0 < a < c_0+pi} a \alpha_i(h) t^{-a+c_0+pi} D_{a0} \right);$$

- the congruence $(\text{id}_{\mathcal{L}} \otimes h)e \equiv e \bmod \mathcal{N}(1)$ implies that $\tilde{e} \equiv e \bmod \mathcal{N}(1)$ and $c, \sigma c \in \mathcal{N}(1)$;

- the congruence

$$(-\sigma c) \circ (\text{id}_{\mathcal{L}} \otimes h)e \circ c \equiv (c - \sigma c) + e + e_1 \bmod \mathcal{N}(2) + t^{c_0} \tilde{\mathcal{N}}^{(2)},$$

where $\tilde{\mathcal{N}}^{(2)} := \sum_{s \geq 2} t^{-sc_0} (\mathcal{L}(s) \cap C_2(\mathcal{L}))_m$ (use that $[\mathcal{N}(1), \mathcal{N}(1)] \subset \mathcal{N}(2)$ and $[\mathcal{N}(1), \mathcal{N}] \subset t^{c_0} \tilde{\mathcal{N}}^{(2)}$) implies $c - \sigma c \in \mathcal{L}_m \bmod \mathcal{N}(2)$ and

$$\tilde{e} \equiv \sum_{a \in \mathbb{Z}^+(p)} t^{-a} \left(D_{a0} - a \sum_{i \geq 0} \alpha_i(h) D_{a+c_0+pi,0} \right) + \alpha_0 D_0 \bmod \mathcal{N}(2) + t^{c_0} \tilde{\mathcal{N}}^{(2)}.$$

It remains to note that this congruence is equivalent to the statement of our lemma. \square

2.4. **The group \mathcal{G}_h .** Let $\mathcal{G}_h = \tilde{\mathcal{G}}_h / \tilde{\mathcal{G}}_h^p C_p(\tilde{\mathcal{G}}_h)$.

Proposition 2.5. *Exact sequence (2.3) induces the following exact sequence of p -groups*

$$(2.5) \quad 1 \longrightarrow G(\mathcal{L})/G(\mathcal{L}(p)) \longrightarrow \mathcal{G}_h \longrightarrow \langle h \rangle \bmod \langle h^p \rangle \longrightarrow 1$$

Proof. Set

$$\begin{aligned} \mathcal{M} &:= \mathcal{N} + \mathcal{L}(p)_{\mathcal{K}} = \sum_{1 \leq s < p} t^{-sc_0} \mathcal{L}(s)_{\mathfrak{m}} + \mathcal{L}(p)_{\mathcal{K}} \\ \mathcal{M}_{<p} &:= \sum_{1 \leq s < p} t^{-sc_0} \mathcal{L}(s)_{\mathfrak{m}_{<p}} + \mathcal{L}(p)_{\mathcal{K}_{<p}} \end{aligned}$$

where $\mathfrak{m}_{<p}$ is the maximal ideal of the valuation ring of $\mathcal{K}_{<p}$.

Then \mathcal{M} has induced structure of a Lie \mathbb{F}_p -algebra (use the Lie bracket from $\mathcal{L}_{\mathcal{K}}$) and for $i \geq 0$, $\mathcal{M}(i) := t^{ic_0} \mathcal{M}$ is a decreasing filtration of ideals in \mathcal{M} . Note that $e \in \mathcal{M}$.

Similarly, $\mathcal{M}_{<p}$ is a Lie \mathbb{F}_p -algebra (containing \mathcal{M} as its subalgebra) and for $i \geq 0$, $\mathcal{M}_{<p}(i) := t^{ic_0} \mathcal{M}_{<p}$ is a decreasing filtration of ideals in $\mathcal{M}_{<p}$, $\mathcal{M}_{<p}(i) \cap \mathcal{M} = \mathcal{M}(i)$.

We have a natural embedding of $\bar{\mathcal{M}} := \mathcal{M}/\mathcal{M}(p-1)$ into $\bar{\mathcal{M}}_{<p} := \mathcal{M}_{<p}/\mathcal{M}_{<p}(p-1)$, and the induced decreasing filtrations of ideals $\bar{\mathcal{M}}(i)$ and $\bar{\mathcal{M}}_{<p}(i)$, where $\bar{\mathcal{M}}(p-1) = \bar{\mathcal{M}}_{<p}(p-1) = 0$, are compatible with this embedding.

Note that for all $i \geq 0$, we have also $(\text{id}_{\mathcal{L}} \otimes h - \text{id}_{\mathcal{M}})^i \mathcal{M} \subset \mathcal{M}(i)$.

Lemma 2.6. $f, \sigma f \in \mathcal{M}_{<p}$.

Proof. Prove by induction on $1 \leq s \leq p$ that $f, \sigma f \in \mathcal{M}_{<p} + \mathcal{L}(s)_{\mathcal{K}_{<p}}$.

If $s = 1$ then $f \in \mathcal{L}_{\mathcal{K}_{<p}} = \mathcal{M}_{<p} + \mathcal{L}(1)_{\mathcal{K}_{<p}}$.

Suppose $1 \leq s_0 < p$ and $f, \sigma f \in \mathcal{M}_{<p} + \mathcal{L}(s_0)_{\mathcal{K}_{<p}}$.

For $1 \leq s \leq s_0 + 1$ let $j_s = \text{rk}_{\mathbb{F}_p}(\mathcal{L}/\mathcal{L}(s))$. Then $0 = j_1 < j_2 < \dots < j_{s_0+1}$. Let $l_1, \dots, l_{j_{s_0+1}} \in \mathcal{L}$ be such that for all $1 \leq s \leq s_0 + 1$, $l_{j_s+1}, \dots, l_{j_{s_0+1}}$ give an \mathbb{F}_p -basis of $\mathcal{L}(s)$ modulo $\mathcal{L}(s_0 + 1)$. This means that for all such s , the elements $l_{j_s+1}, \dots, l_{j_{s_0+1}}$ form \mathbb{F}_p -basis of $\mathcal{L}(s)$ modulo $\mathcal{L}(s_0 + 1)$.

With above notation for $1 \leq j \leq j_{s_0+1}$, there are unique $b_j \in \mathcal{K}_{<p}$ such that $f \equiv \sum_j b_j l_j \bmod \mathcal{L}(s_0 + 1)_{\mathcal{K}_{<p}}$. By inductive assumption, if $s < s_0$ and $l_j \in \mathcal{L}(s) \setminus \mathcal{L}(s_0 + 1)$ then $b_j, \sigma b_j \in \mathfrak{m}_{<p} t^{-c_0 s}$ and we must prove that if $l_j \in \mathcal{L}(s_0)$ then $b_j \in \mathfrak{m}_{<p} t^{-c_0 s_0}$.

Let $e \circ f = e + f + X(f, e)$. Then $X(f, e) \in \mathcal{M}_{<p} + \mathcal{L}(s_0 + 1)_{\mathcal{K}_{<p}}$ (use that $e \in \mathcal{M}_{<p}$ and $[\mathcal{M}_{<p}, \mathcal{L}(s_0)_{\mathcal{K}_{<p}}] \subset \mathcal{L}(s_0 + 1)_{\mathcal{K}_{<p}}$) and, therefore, $\sigma f - f \in \mathcal{M}_{<p} + \mathcal{L}(s_0 + 1)_{\mathcal{K}_{<p}}$.

Thus, $\sigma f - f \equiv \sum_j a_j l_j$, where for all $s \leq s_0$ and $j_s < j \leq j_{s_0+1}$, we have $a_j \in \mathfrak{m}_{<p} t^{-c_0 s}$. In particular, for the indices $j_{s_0} < j \leq j_{s_0+1}$, we have $\sigma b_j - b_j \in \mathfrak{m}_{<p} t^{-c_0 s_0}$. Therefore,

$$\sigma(b_j t^{c_0 s_0/p}) - t^{c_0 s_0(1-1/p)} (b_j t^{c_0 s_0/p}) \in \mathfrak{m}_{<p},$$

and this implies that $b_j t^{c_0 s_0/p} \in \mathfrak{m}_{< p}$ and $\sigma b_j, b_j \in \mathfrak{m}_{< p} t^{-c_0 s_0}$. Lemma 2.6 is proved. \square

Consider the orbit of $\bar{f} := f \bmod \mathcal{M}_{< p}(p-1)$ with respect to the natural action of $\tilde{\mathcal{G}}_h \subset \text{Aut } \mathcal{K}_{< p}$ on $\bar{\mathcal{M}}_{< p}$. Prove that the stabilizer \mathcal{H} of \bar{f} equals $\tilde{\mathcal{G}}_h^p C_p(\tilde{\mathcal{G}}_h)$.

If $l \in G(\mathcal{L})$ then the corresponding element of $\mathcal{G}_{< p}$ sends f to $f \circ l$. This means that if $l \in \mathcal{H} \cap G(\mathcal{L})$ then (use that $\mathcal{M}(p-1) \subset \mathcal{L}_m + \mathcal{L}(p)_\mathcal{K}$)

$$l \in \mathcal{M}_{< p}(p-1) \cap \mathcal{L} = \mathcal{M}(p-1) \cap \mathcal{L} = \mathcal{L}(p)_\mathcal{K} \cap \mathcal{L} = \mathcal{L}(p) = C_p(\tilde{\mathcal{G}}_h).$$

Therefore, $\mathcal{H} \cap G(\mathcal{L}) = C_p(\tilde{\mathcal{G}}_h) \subset \mathcal{H}$ and we have the induced embedding $\kappa : G(\mathcal{L})/G(\mathcal{L}(p)) \rightarrow \tilde{\mathcal{G}}_h/\mathcal{H}$.

Note that $\tilde{\mathcal{G}}_h^p \bmod C_p(\tilde{\mathcal{G}}_h)$ is generated by $h_{< p}^p$. This follows from the fact that any finite p -group of nilpotent class $< p$ is P -regular, cf. [18] Subsections 12.3-12.4. In particular, for any $g \in G(\mathcal{L})$,

$$(h_{< p} \circ g)^p \equiv h_{< p}^p \circ g' \bmod C_p(\tilde{\mathcal{G}}_h),$$

where g' is the product of p -th powers of elements from $G(\mathcal{L})$, but $G(\mathcal{L})$ has period p .

Recall that $(\text{id}_\mathcal{L} \otimes h_{< p})(f) = c \circ (A \otimes \text{id}_{\mathcal{K}_{< p}})f$, where $c \in \mathcal{L}_\mathcal{K}$ and $A = \text{Ad}(h_{< p})$ is an automorphism \mathcal{L} . Then $h_{< p}^p(f)$ is equal to

$$(\text{id}_\mathcal{L} \otimes h)^{p-1} (c \circ (A \otimes h^{-1})c \circ \dots \circ (A \otimes h^{-1})^{p-1}c) \circ (A^p \otimes \text{id}_{\mathcal{K}_{< p}})f.$$

Clearly, $(A - \text{id}_\mathcal{L})^p \mathcal{L} \subset \mathcal{L}(p)$ and, therefore, $(A^p \otimes \text{id}_{\mathcal{K}_{< p}})\bar{f} = \bar{f}$.

Similarly, $B = A \otimes h^{-1}$ is an automorphism of the Lie \mathbb{F}_p -algebra \mathcal{N} and for all $i \geq 0$, $(B - \text{id}_\mathcal{N})\mathcal{N}(i) \subset \mathcal{N}(i+1)$. Note that $c \in \mathcal{N}(1)$, cf. Subsection 2.3.

Lemma 2.7. *For any $m \in \mathcal{N}(1)$, $m \circ B(m) \circ \dots \circ B^{p-1}m \in \mathcal{N}(p)$.*

Proof. Consider the Lie algebra $\mathfrak{M} = \mathcal{N}(1)/\mathcal{N}(p)$ with the filtration $\{\mathfrak{M}(i)\}_{i \geq 1}$ induced by the filtration $\{\mathcal{N}(i)\}_{i \geq 1}$. This filtration is central, i.e. for any $i, j \geq 1$, $[\mathfrak{M}(i), \mathfrak{M}(j)] \subset \mathfrak{M}(i+j)$. In particular, the nilpotent class of \mathfrak{M} is $< p$.

The operator B induces the operator on \mathfrak{M} which we denote also by B . Clearly, $B = \widetilde{\exp} \mathcal{B}$ where \mathcal{B} is a differentiation on \mathfrak{M} such that for all $i \geq 1$, $\mathcal{B}(\mathfrak{M}(i)) \subset \mathfrak{M}(i+1)$.

Let $\widetilde{\mathfrak{M}}$ be a semi-direct product of \mathfrak{M} and the trivial Lie algebra $\mathbb{F}_p w$ via \mathcal{B} . This means that $\widetilde{\mathfrak{M}} = \mathfrak{M} \oplus \mathbb{F}_p w$ as \mathbb{F}_p -module, \mathfrak{M} and $\mathbb{F}_p w$ are Lie subalgebras of $\widetilde{\mathfrak{M}}$ and for any $m \in \mathfrak{M}$, $[w, m] = \mathcal{B}(m)$. Clearly, $C_2(\widetilde{\mathfrak{M}}) = [\widetilde{\mathfrak{M}}, \widetilde{\mathfrak{M}}] \subset \mathfrak{M}(2)$. This implies that $\widetilde{\mathfrak{M}}$ has nilpotent class $< p$ and we can consider the p -group $G(\widetilde{\mathfrak{M}})$. This group has nilpotent class $< p$ and period p (because for any $\bar{m} \in \widetilde{\mathfrak{M}}$, its p -th power in $G(\widetilde{\mathfrak{M}})$ equals $p\bar{m} = 0$).

Note that the conjugation by w in $G(\widetilde{\mathfrak{M}})$ is given by the automorphism $\widetilde{\exp} \mathcal{B} = B$. In particular, for any element $\bar{m} = m \bmod \mathcal{N}(p) \in \mathfrak{M}$, we have $w \circ \bar{m} = B(\bar{m}) \circ w$. Therefore, $0 = (\bar{m} \circ w)^p = \bar{m} \circ B(\bar{m}) \circ \dots \circ B^{p-1}(\bar{m}) \circ w^p$, and it remains to note that $w^p = 0$. \square

Applying the above Lemma we obtain that

$$c \circ (A \otimes h^{-1})c \circ \dots \circ (A \otimes h^{-1})^{p-1}c \in \mathcal{L}(p)_{\mathcal{K}} \subset \mathcal{M}(p-1)$$

and, therefore, $h_{<p}^p(\bar{f}) = 0$.

Thus, we proved that $\widetilde{\mathcal{G}}_h^p C_p(\widetilde{\mathcal{G}}_h) \subset \mathcal{H}$.

Suppose $g = h_{<p}^m l \in \mathcal{H}$ with some $l \in G(\mathcal{L})$. Then we have

$$g(f) \equiv f \bmod \mathcal{M}_{<p}(p-1).$$

This congruence in the Lie algebra $\mathcal{M}_{<p}$ can be replaced by the equivalent congruence $g(f) \equiv f \bmod G(\mathcal{M}_{<p}(p-1))$ in the corresponding p -group $G(\mathcal{M}_{<p}(p-1))$. (Use that $\mathcal{M}_{<p}(p-1)$ is an ideal in $\mathcal{M}_{<p}$ and the embedding of Lie algebras $\mathcal{M}_{<p}(p-1) \subset \mathcal{M}_{<p}$ is at the same time the embedding of the appropriate p -groups.). Therefore, $g(f) = b \circ f$ where $b \in \mathcal{M}_{<p}(p-1)$. Note that for obvious reasons $\sigma(b) \in \mathcal{M}_{<p}(p-1)$. Then the equality

$$g(e) \circ b \circ f = g(e) \circ g(f) = g(\sigma f) = \sigma b \circ \sigma f = \sigma b \circ e \circ f$$

implies that $g(e) \equiv e \bmod \mathcal{M}(p-1)$ and we obtain

$$(\text{id} \otimes h)^m(e) \equiv e \bmod \mathcal{M}(p-1).$$

Clearly, $\mathcal{L}_m + \mathcal{L}(p)_{\mathcal{K}} \supset \mathcal{M}(p-1)$ and, therefore, for the element

$$e_{<p} = \sum_{a \in \mathbb{Z}^0(p) \cap [0, (p-1)c_0]} t^{-a} D_{a0}$$

we obtain $(\text{id}_{\mathcal{L}} \otimes h^m)e_{<p} \equiv e_{<p} \bmod \mathcal{L}_m$.

This means for all $a \in \mathbb{Z}^0(p) \cap [0, (p-1)c_0]$, $h^m(t^{-a}) \equiv t^{-a} \bmod m$, and we obtain that $m \equiv 0 \bmod p$ (take e.g. $a = c_0 + 1$).

Therefore, $l \in \mathcal{H} \cap G(\mathcal{L}) = C_p(\widetilde{\mathcal{G}}_h)$ and $\mathcal{H} \subset \widetilde{\mathcal{G}}_h^p C_p(\widetilde{\mathcal{G}}_h)$.

Finally, $\widetilde{\mathcal{G}}_h/\mathcal{H} = \mathcal{G}_h$ and it remains to note that $\mathcal{H} \bmod C_p(\widetilde{\mathcal{G}}_h) = \langle h_{<p}^p \rangle$ and, therefore, $\text{Coker} \kappa = \langle h \rangle \bmod \langle h^p \rangle$. \square

Corollary 2.8. *If L_h is a Lie algebra over \mathbb{F}_p such that $\mathcal{G}_h = G(L_h)$ then (2.5) induces the following short exact sequence of Lie \mathbb{F}_p -algebras*

$$0 \longrightarrow \mathcal{L}/\mathcal{L}(p) \longrightarrow L_h \longrightarrow \mathbb{F}_p h \longrightarrow 0$$

2.5. Ramification estimates. Use the identification from Subsection 1.3, $\eta_0 : \text{Gal}(\mathcal{K}_{<p}/\mathcal{K}) \simeq G(\mathcal{L})$ and set for $s \in \mathbb{N}$, $\mathcal{K}[s] := \mathcal{K}_{<p}^{G(\mathcal{L}(s+1))}$. Note that $\mathcal{K}[s]/\mathcal{K}$ is Galois and its Galois group is $G(\mathcal{L}/\mathcal{L}(s+1))$.

Denote by $v[s]$ the maximal upper ramification number of the extension $\mathcal{K}[s]/\mathcal{K}$. In other words,

$$v[s] = \max\{v \mid \Gamma_{\mathcal{K}}^{(v)} \text{ acts non-trivially on } \mathcal{K}[s]\}.$$

Proposition 2.9. *For all $s \in \mathbb{N}$, $v[s] = c_0 s - 1$.*

Proof. Recall that for any $v \geq 0$, $\pi_f(e)(\mathcal{G}^{(v)}) = \mathcal{L}^{(v)}$ and for a sufficiently large N , the ideal $\mathcal{L}_k^{(v)}$ is generated by all $\sigma^n \mathcal{F}_{\gamma, -N}^0$, where $\gamma \geq v$, $n \in \mathbb{Z}$ and the elements $\mathcal{F}_{\gamma, -N}^0$ were given in Subsection 1.4.

Note that $\mathcal{L}_k^{(v)}$ is contained in the ideal generated by the monomials $\sigma^n[\dots[D_{a_1 \bar{n}_1}, D_{a_2 \bar{n}_2}], \dots, D_{a_r \bar{n}_r}]$ such that $\max\{n_1, \dots, n_r\} = 0$ and $a_1 p^{n_1} + \dots + a_r p^{n_r} \geq v$. So,

$$v \leq a_1 + \dots + a_r \leq c_0 \text{wt}([\dots[D_{a_1 \bar{n}_1}, D_{a_2 \bar{n}_2}], \dots, D_{a_r \bar{n}_r}]) - r_0,$$

where r_0 is the number of non-zero a_i 's.

If $v > c_0 s - 1$ then $\text{wt}([\dots[D_{a_1 \bar{n}_1}, D_{a_2 \bar{n}_2}], \dots, D_{a_r \bar{n}_r}]) > s$ and we have $\mathcal{L}^{(v)} \subset \mathcal{L}(s+1)$.

If $v = c_0 s - 1$ then $\text{wt}([\dots[D_{a_1 \bar{n}_1}, D_{a_2 \bar{n}_2}], \dots, D_{a_r \bar{n}_r}]) \leq s$ iff $r_0 = 1$ and the only non-zero a_i equals $c_0 s - 1$. Therefore, $\mathcal{L}_k^{(v)} \bmod \mathcal{L}_k(s+1)$ is generated by the images of $D_{c_0 s - 1, \bar{n}}$, $\bar{n} \in \mathbb{Z}/N_0$, and $\mathcal{L}^{(v)} \not\subset \mathcal{L}(s+1)$. \square

3. STRUCTURE OF L_h

By proposition 2.5, the group structure of $\mathcal{G}_h = G(L_h)$ is given via the conjugation $\text{Ad}(h_{<p})$ on $G(\mathcal{L}/\mathcal{L}(p))$, where $h_{<p}$ is a chosen lift of h (the short exact sequence from Proposition 2.5 obviously admits a section). This conjugation appears as a unipotent automorphism of the Lie algebra $\mathcal{L}/\mathcal{L}(p)$ and we can introduce a differentiation $\text{adh}_{<p}$ of $\mathcal{L}/\mathcal{L}(p)$ by the relation $\text{Ad}(h_{<p}) = \widetilde{\exp}(\text{ad}(h_{<p}))$, where $\widetilde{\exp}$ is the truncated exponential, cf. Subsection 2.1 (use that $\mathcal{L}/\mathcal{L}(p)$ has nilpotent class $< p$). So, the knowledge of the Lie algebra L_h is equivalent to the knowledge of the $\text{ad}(h_{<p})$. Note that $\text{ad}(h_{<p})$ comes from a differentiation of \mathcal{L} and it depends on a choice of the lift $h_{<p}$.

3.1. Interpretation of the action of $\text{id}_{\mathcal{L}} \otimes h$ on $\bar{\mathcal{M}}$. Consider the induced action of $\text{id}_{\mathcal{L}} \otimes h$ on $\bar{\mathcal{M}}$. Recall that $h(t) = t \widetilde{\exp}(\varepsilon^p) \bmod t^{p c_0 + 1}$, where we set

$$\varepsilon^p = \sum_{i \geq 0} A_i(h) t^{c_0 + p i}$$

with all $A_i(h) \in k$, $A_0(h) \neq 0$, cf. Subsection 2.1.

Let \mathcal{H} be a linear continuous operator on $\mathcal{L}_{\mathcal{K}}$ such that for all $a \in \mathbb{Z}$ and $l \in \mathcal{L}_k$, $\mathcal{H}(t^a l) = a t^a \varepsilon^p l$. Then on $\bar{\mathcal{M}}$ we have $\text{id}_{\mathcal{L}} \otimes h = \widetilde{\exp}(\mathcal{H})$ (use that $\mathcal{H}^p = 0$).

Note that if for $0 \leq i < p$, $h_i := \mathcal{H}^i/i! : \bar{\mathcal{M}} \rightarrow \bar{\mathcal{M}}$ and $h_i = 0$ if $i \geq p$ then for any $j \geq 0$, $h_i(\bar{\mathcal{M}}(j)) \subset \bar{\mathcal{M}}(i+j)$ and for any natural n , $(\text{id}_{\mathcal{L}} \otimes h)^n = \sum_{i \geq 0} n^i h_i$. An analogue of these properties will appear below when we describe the action of $\text{id}_{\mathcal{L}} \otimes h_{<p}$ on f .

3.2. General situation. The situation from above Subsection 3.1 can be formalized as follows.

Suppose \mathfrak{M} is an \mathbb{F}_p -module (actually we can assume that \mathfrak{M} is a module over any ring where $(p-1)!$ is invertible). Suppose $g : \mathfrak{M} \rightarrow \mathfrak{M}$ is an automorphism of the \mathbb{F}_p -module \mathfrak{M} such that $g^p = \text{id}_{\mathfrak{M}}$. Assume that

- for any $m \in \mathfrak{M}$, there are $g_i(m) \in \mathfrak{M}$, where $1 \leq i < p$, such that for all $n \geq 0$, $g^n(m) = m + \sum_{1 \leq i < p} g_i(m)n^i$.

Set $g_0(m) = m$ and $g_i(m) = 0$ if $i \geq p$.

Proposition 3.1. *With above notation we have:*

- a) for all $i \geq 0$, $g_i : \mathfrak{M} \rightarrow \mathfrak{M}$ are unique linear morphisms;
- b) for all $i \geq 0$, $g_i(\mathfrak{M}) \subset (g - \text{id}_{\mathfrak{M}})^i(\mathfrak{M})$;
- c) if $i_1, \dots, i_s \geq 0$ then $(g_{i_1} \cdot \dots \cdot g_{i_s})(\mathfrak{M}) \subset (g - \text{id}_{\mathfrak{M}})^{i_1 + \dots + i_s}(\mathfrak{M})$;
- d) the map $g^U = \sum_{i \geq 0} g_i \otimes U^i : \mathfrak{M} \rightarrow \mathfrak{M} \otimes \mathbb{F}_p[[U]]$ determines the action of the formal additive group $\mathbb{G}_a = \text{Spf } \mathbb{F}_p[[U]]$ on \mathfrak{M} ;
- e) if $1 \leq i < p$ then $g_i = g_1^i/i!$ (here $g_1^i = \underbrace{g_1 \cdot \dots \cdot g_1}_{i \text{ times}}$).

Proof. For any $m \in \mathfrak{M}$, $g_1(m), \dots, g_{p-1}(m)$ are unique solutions of the non-degenerate system of equations

$$\sum_{1 \leq i < p} g_i(m)n^i = g^n(m) - m$$

where $n = 1, \dots, p-1$. Therefore, all $g_i(m)$ are unique and depend linearly on m . This proves a).

For $i \geq 0$ and $F \in \mathfrak{M} \otimes \mathbb{F}_p[[U]]$, define the i -th differences $(\Delta^i F)(U) \in \mathfrak{M} \otimes \mathbb{F}_p[[U]]$ by setting $\Delta^0 F = F$ and

$$(\Delta^{i+1} F)(U) = (\Delta^i F)(U+1) - (\Delta^i F)(U).$$

In particular, for $0 \leq j < i$, $\Delta^i(m \otimes U^j) = 0$ and $(\Delta^i)(m \otimes U^i) = i!m$. Therefore, for any $i \geq 0$,

$$(3.1) \quad (\Delta^i g^U(m))|_{U=0} = i!g_i(m) + \sum_{j>i} f_{ij}g_j(m),$$

where all $f_{ij} \in \mathbb{F}_p$. Note that for every value $n_0 \geq 0$,

$$\begin{aligned} (\Delta^1 g^U(m))|_{u=n_0} &= g(g^U(m)|_{u=n_0}) - g^U(m)|_{u=n_0} \in (g - \text{id}_{\mathfrak{M}})(\mathfrak{M}), \\ (\Delta^2 g^U(m))|_{u=n_0} &= g((\Delta^1 g^U(m))|_{u=n_0}) - (\Delta^1 g^U(m))|_{u=n_0} \in (g - \text{id}_{\mathfrak{M}})^2(\mathfrak{M}) \end{aligned}$$

and so on. Therefore, for any $i \geq 0$,

$$(\Delta^i g^U)(m)|_{U=n_0} \in (g - \text{id}_{\mathfrak{M}})^i \mathfrak{M}.$$

Then (3.1) implies (use $i = p-1$) that $g_{p-1}(m) \in (g - \text{id}_{\mathfrak{M}})^{p-1}(\mathfrak{M})$ and then by descending induction on i that $g_i(m) \in (g - \text{id}_{\mathfrak{M}})^i(\mathfrak{M})$. This proves b).

In c) use induction on s . The case $s = 1$ is proved in b). If $s > 1$ then we must prove with $j = i_2 + \dots + i_s$ that

$$g_{i_1}((g - \text{id}_{\mathfrak{M}})^j \mathfrak{M}) \subset (g - \text{id}_{\mathfrak{M}})^{i_1+j} \mathfrak{M}.$$

This can be obtained from a) by replacing \mathfrak{M} to $(g - \text{id}_{\mathfrak{M}})^j \mathfrak{M}$.

For any natural numbers n_1, n_2 the relation $g^{n_1+n_2}(m) = g^{n_2}(g^{n_1}(m))$ means that

$$\sum_{0 \leq i < p} (n_1 + n_2)^i g_i = \sum_{0 \leq i_1, i_2 < p} n_2^{i_2} n_1^{i_1} g_{i_2} \circ g_{i_1},$$

and implies that we have the appropriate identity of formal power series

$$(g^U \otimes \text{id}_{\mathbb{G}_a}) \circ g^U = (\text{id}_{\mathfrak{M}} \otimes \Delta_{\mathbb{G}_a}) \circ g^U,$$

with the coaddition $\Delta = \Delta_{\mathbb{G}_a}$ in \mathbb{G}_a such that $\Delta(U) = U \otimes 1 + 1 \otimes U$. This proves d).

If $i \geq 1$ the above identity for g^U implies the identity

$$(g^U \otimes \text{id}_{\mathbb{G}_a^i}) \circ \dots \circ (g^U \otimes \text{id}_{\mathbb{G}_a}) \circ g^U = (\text{id}_{\mathfrak{M}} \otimes \Delta^{(i)}) \circ g^U,$$

where $\Delta^{(i)} = (\Delta \otimes \text{id}_{\mathbb{G}_a^{i-1}}) \circ \dots \circ (\Delta \otimes \text{id}_{\mathbb{G}_a}) \circ \Delta$ is the i -th coaddition $\mathbb{F}_p[[U]] \rightarrow \mathbb{F}_p[[U]]^{\otimes i}$ for \mathbb{G}_a . Then e) can be obtained by comparing the coefficients for $U^{\otimes i}$ in this identity. \square

Definition. $dg^U := g_1 \otimes U : \mathfrak{M} \rightarrow \mathfrak{M} \otimes U$ is the differential of g .

By above Proposition 3.1e) the action of g on \mathfrak{M} can be uniquely recovered from its differential dg^U .

3.3. Auxiliary statement. Assume that \mathfrak{L} is a Lie algebra over \mathbb{F}_p . Let $\mathcal{A} = \mathcal{A}(\mathfrak{L})$ be the enveloping algebra of \mathfrak{L} . Then we have a canonical embedding $\mathfrak{L} \rightarrow \mathcal{A}$. Provide \mathcal{A} with a standard structure of coalgebra $\Delta : \mathcal{A} \rightarrow \mathcal{A} \otimes \mathcal{A}$ by setting $\Delta(l) = l \otimes 1 + 1 \otimes l$ for all $l \in \mathfrak{L}$.

Let $J = J(\mathfrak{L})$ be the augmentation ideal of \mathcal{A} generated by all $l \in \mathfrak{L}$. Note that $\mathcal{A} \otimes \mathcal{A}$ can be identified with the enveloping algebra of $\mathfrak{L} \oplus \mathfrak{L}$ and the appropriate augmentation ideal equals $J(\mathfrak{L} \oplus \mathfrak{L}) = J \otimes \mathcal{A} + \mathcal{A} \otimes J$.

Suppose \mathfrak{L} has nilpotent class $< p$. Then we have the following interpretation of the Campbell-Hausdorff operation \circ on \mathfrak{L} in the enveloping algebra \mathcal{A} :

- $\mathfrak{L} = \{a \in \mathcal{A} \bmod J(\mathfrak{L})^p \mid \Delta a \equiv a \otimes 1 + 1 \otimes a \bmod J(\mathfrak{L} \oplus \mathfrak{L})^p\}$;
 - the truncated exponential $\widetilde{\exp}$ establishes a group isomorphism $\iota : G(\mathfrak{L}) \rightarrow \mathcal{D}(\mathfrak{L})$, where
- $$\mathcal{D}(\mathfrak{L}) = \{a \in (1 + J(\mathfrak{L}))^\times \bmod J(\mathfrak{L})^p \mid \Delta a \equiv a \otimes a \bmod J(\mathfrak{L} \oplus \mathfrak{L})^p\}$$

is the group of “diagonal elements of \mathcal{A} modulo degree p ” with respect to the operation induced by the multiplication in \mathcal{A} ;

- $\iota^{-1} : \mathcal{D}(\mathfrak{L}) \longrightarrow G(\mathfrak{L})$ is given via the truncated logarithm $\widetilde{\log}$.

These properties easily follow from the explicit construction of a basis in \mathcal{A} from basis of \mathfrak{L} given by the Poincare-Birkhoff-Witt theorem, cf. [Ab1].

Suppose \mathfrak{L} is provided with a decreasing filtration of ideals $\{\mathfrak{L}^i\}_{i \geq 0}$ such that $\mathfrak{L}^0 = \mathfrak{L}$ and $\mathfrak{L}^i = 0$ if $i \geq p$. Define the weight function on \mathfrak{L} by setting $\text{wt}^*(0) = \infty$ and $\text{wt}^*(l) = i$ if $l \in \mathfrak{L}^i \setminus \mathfrak{L}^{i+1}$.

Assume in addition that the filtration $\{\mathfrak{L}^i\}$ is “central”, i.e. for any $i, j \geq 0$, $[\mathfrak{L}^i, \mathfrak{L}^j] \subset \mathfrak{L}^{i+j}$. (We shall specify below $\mathfrak{L}^i = \bar{\mathcal{M}}(i)$ for $0 \leq i < p$.)

Suppose $\{l_i \mid 1 \leq i \leq r\}$ is an \mathbb{F}_p -basis of \mathfrak{L} and this basis is compatible with the filtration $\{\mathfrak{L}^i\}_{i \geq 0}$, i.e. there are $0 = j_0 \leq j_1 \leq \dots \leq j_p = r$ such that for any $i \geq 0$, $\{l_j \mid j_i < j \leq r\}$ is an \mathbb{F}_p -basis of \mathfrak{L}^i . Then by the Poincare-Birkhoff-Witt theorem

$$\{l_{i_1} \dots l_{i_s} \mid s \geq 0, i_1 \leq i_2 \leq \dots \leq i_s\}$$

is an \mathbb{F}_p -basis of \mathcal{A} . Extend wt^* to \mathcal{A} by setting for every non-zero \mathbb{F}_p -linear combination,

$$\text{wt}^* \left(\sum_{i_1, \dots, i_s} \alpha_{i_1 \dots i_s} l_{i_1} \dots l_{i_s} \right) = \min \{ \text{wt}^*(l_{i_1}) + \dots + \text{wt}^*(l_{i_s}) \mid \alpha_{i_1 \dots i_s} \neq 0 \}.$$

Let $\mathcal{A}^i = \{a \in \mathcal{A} \mid \text{wt}^*(a) \geq i\}$. Then for any $i, j \geq 0$, $\mathcal{A}^i \mathcal{A}^j \subset \mathcal{A}^{i+j}$ (use that $\{\mathfrak{L}^i\}$ is “central”). In particular, $\{\mathcal{A}^i\}_{i \geq 0}$ is a decreasing filtration of ideals of \mathcal{A} . Obviously, $\mathcal{A}^i \cap \mathfrak{L} = \mathfrak{L}^i$.

Let B be a \mathbb{Z}_p -linear operator on \mathfrak{L} such that for any $l \in \mathfrak{L}^i$, $B(l) \equiv l \pmod{\mathfrak{L}^{i+1}}$. For $l \in \mathfrak{L}$ and $n \in \mathbb{N}$, set in the appropriate p -group $G(L)$, $l[n] := l \circ B(l) \circ \dots \circ B^{n-1}(l)$.

Proposition 3.2. *Suppose $l \in \mathfrak{L}^1$. For $1 \leq i \leq p-1$ there are (unique) $l_i \in \mathfrak{L}^i$ such that for any $n \geq 0$, $l[n] = l_1 n + l_2 n^2 + \dots + l_{p-1} n^{p-1}$.*

Proof. Prove the existence of $l_i \in \mathfrak{L}^i$. (For the uniqueness of l_i , cf. Proposition 3.1c.)

Clearly, $B = \widetilde{\exp}(\mathcal{B})$, where \mathcal{B} is a linear operator on \mathfrak{L} such that for all i , $\mathcal{B}(\mathfrak{L}^i) \subset \mathfrak{L}^{i+1}$. If for $0 \leq i \leq p-1$, $l'_i = \mathcal{B}^i(l)/i!$ then $l'_i \in \mathfrak{L}^{i+1}$ and for any $m \geq 0$, $B^m(l) = \widetilde{\exp}(m\mathcal{B})(l) = \sum_{i \geq 0} l'_i m^i$. (We set $0^0 = 1$.)

Let $\mathcal{E} : \mathfrak{L} \longrightarrow \mathcal{A}$ be the map given by the truncated exponential. Then for $i \geq 0$, there are $d_i \in \mathcal{A}^{i+1}$ such that for any $m \geq 0$,

$$\mathcal{E}(B^m(l)) = 1 + \sum_{i \geq 0} d_i m^i.$$

Therefore, $\mathcal{E}(l)\mathcal{E}(B(l))\dots\mathcal{E}(B^{n-1}(l)) =$

$$1 + \sum_{\substack{1 \leq s \leq n \\ i_1, \dots, i_s \geq 0}} \left(\sum_{0 \leq m_1 < \dots < m_s < n} m_1^{i_1} \dots m_s^{i_s} \right) d_{i_1} \dots d_{i_s}.$$

Let $d(i_1, \dots, i_s) := i_1 + \dots + i_s + s$ and

$$\sum_{0 \leq m_1 < \dots < m_s < n} m_1^{i_1} \dots m_s^{i_s} = f_{i_1 \dots i_s}(n).$$

Note that $d_{i_1} \dots d_{i_s} \in \mathcal{A}^{d(i_1 + \dots + i_s)}$.

Lemma 3.3. *If $s \geq 1$, $i_1, \dots, i_s \geq 0$ and $d(i_1, \dots, i_s) < p$ then there are polynomials $F_{i_1 \dots i_s} \in \mathbb{Z}_p[U]$ such that:*

- a) *for all n , $F_{i_1 \dots i_s}(n) = f_{i_1 \dots i_s}(n)$;*
- b) *$F_{i_1 \dots i_s}(0) = 0$;*
- c) *$\deg F_{i_1 \dots i_s} = d(i_1, \dots, i_s)$.*

Proof of Lemma. First, consider the case $s = 1$.

Apply induction on i_1 .

If $i_1 = 0$ then $f_0(n) = n$ and we can take $F_0 = U$.

Suppose $i_1 \geq 1$, $d(i_1) < p$ (i.e. $0 \leq i_1 \leq p-2$) and our Lemma is proved for all indices $j < i_1$.

For any $m < n$ we have,

$$(m+1)^{i_1+1} - m^{i_1+1} = \sum_{0 \leq j \leq i_1} C_j(i_1) m^j,$$

where all $C_j(i) \in \mathbb{Z}_p$. Therefore, for any $n \geq 0$,

$$n^{i_1+1} = \sum_{0 \leq j \leq i_1} C_j(i_1) f_j(n) = \sum_{0 \leq j < i_1} C_j(i_1) F_j(n) + (i_1 + 1) f_{i_1}(n)$$

and we obtain $F_{i_1}(U) = (i_1 + 1)^{-1} \left(U^{i_1+1} - \sum_{0 \leq j < i_1} C_j(i_1) F_j(U) \right)$. Clearly, the degree of F_{i_1} equals $i_1 + 1 = d(i_1)$ and $F_{i_1}(0) = 0$. The case $s = 1$ is considered.

Suppose $s > 1$ and use induction on s . Then for any $m < n$,

$$f_{i_1 \dots i_s}(m+1) - f_{i_1 \dots i_s}(m) = \sum_{0 \leq m_1 < \dots < m_s = m} m_1^{i_1} \dots m_s^{i_s} = m^{i_s} F_{i_1 \dots i_{s-1}}(m).$$

Suppose $F_{i_1 \dots i_{s-1}}(U) = \sum_{j \leq d(i_1, \dots, i_{s-1})} C_j(i_1, \dots, i_{s-1}) U^j$. Then for any $n \geq 1$ (note that $d(i_1, \dots, i_s) - 1 = d(i_1, \dots, i_{s-1})$),

$$f_{i_1 \dots i_s}(n) = \sum_{i_s \leq j \leq d(i_1, \dots, i_s) - 1} C_j(i_1, \dots, i_{s-1}) F_j(n),$$

and we can take $F_{i_1 \dots i_s} = \sum_{i_s \leq j \leq d(i_1, \dots, i_s) - 1} C_j(i_1, \dots, i_{s-1}) F_j$. Clearly, the degree of $F_{i_1 \dots i_s}$ equals $d(i_1, \dots, i_s)$ and $F_{i_1 \dots i_s}(0) = 0$. \square

The above lemma implies that for all $n \geq 1$,

$$\mathcal{E}(l[n]) = 1 + \sum_{1 \leq i \leq p-1} d'_i n^i + a(l, n),$$

where all $d'_i \in \mathcal{A}^i$ and $a(l, n) \in \mathcal{A}^p + J(\mathfrak{L})^p$. Applying to this equality the truncated logarithm we obtain that $l[n] = l_1 n + \dots + l_{p-1} n^{p-1} + b(l, n)$, where all $l_i \in \mathcal{A}^i \cap \mathfrak{L} = \mathfrak{L}^i$ and $b(l, n) \in (\mathcal{A}^p + J(\mathfrak{L})^p) \cap \mathfrak{L} = 0$. The proposition is proved. \square

As a matter of fact, the proof of Proposition 3.2 gives the following result:

• If $i^0 \geq 1$ and $l \in \mathfrak{L}^{i^0}$ then for $i^0 \leq i \leq p-1$ there unique $l_i \in \mathfrak{L}^i$ such that for any $n \geq 0$, $l[n] = l_{i^0} n + \dots + l_{p-1} n^{p-i^0}$.

We should formally follow the above proof of Proposition 3.1. Then $l \in \mathfrak{L}^{i^0}$ implies that all $l'_i \in \mathfrak{L}^{i+i^0}$, $d_i \in \mathcal{A}^{i+i^0}$. Lemma 3.3 remains unchanged and, finally, all $d'_i \in \mathcal{A}^{i+i^0-1}$ and all $l_i \in \mathcal{A}^{i+i^0-1} \cap \mathfrak{L} = \mathfrak{L}^{i+i^0-1}$ if $i \leq p-i^0$.

This allows us to state the following result.

Proposition 3.4. *There are linear maps $\pi_i : \mathfrak{L}^1 \rightarrow \mathfrak{L}^1$ such that for any $j \geq 0$, $\pi_i(\mathfrak{L}^j) \subset \mathfrak{L}^{i+j-1}$ (in particular, $\pi_i = 0$ if $i \geq p$) and for any $l \in \mathfrak{L}^1$ and $n \in \mathbb{N}$, $l[n] = \sum_i \pi_i(l) n^i$.*

3.4. Lie algebra $\bar{\mathcal{M}}^f$ and the action of $\text{id}_{\mathcal{L}} \otimes h_{<p}$. Here we study the action of the lift $\text{id}_{\mathcal{L}} \otimes h_{<p}$ of $\text{id}_{\mathcal{L}} \otimes h$ on $\bar{f} = f \bmod \mathcal{M}_{<p}(p-1) \in \bar{\mathcal{M}}_{<p}$.

As earlier, $(\text{id}_{\mathcal{L}} \otimes h_{<p})(\bar{f}) = \bar{c} \circ (A \otimes \text{id}_{\mathcal{K}_{<p}}) \bar{f}$, where we set $\bar{c} = c \bmod \mathcal{M}(p-1) \in \bar{\mathcal{M}}(1)$ and $A = \text{Ad}h_{<p} = \widetilde{\text{exp}}(\text{adh}_{<p})$. For $n \in \mathbb{N}$, let

$$(3.2) \quad (\text{id}_{\mathcal{L}} \otimes h_{<p}^n)(f) = c(n) \circ f(n),$$

where $c(n) = (\text{id}_{\mathcal{L}} \otimes h_{<p}^{n-1})(c \circ (A \otimes h^{-1})c \circ \dots \circ (A \otimes h^{-1})^{n-1}c)$ and $f(n) = (A^n \otimes \text{id}_{\mathcal{K}_{<p}})f$.

Clearly, $f(n) \equiv \sum_{i \geq 0} f^{(i)} n^i \bmod \mathcal{M}_{<p}(p-1)$, where $f^{(0)} = f$ and all $f^{(i)} = (\text{adh}_{<p} \otimes \text{id}_{\mathcal{K}_{<p}})^i(f)/i! \in (A \otimes \text{id}_{\mathcal{K}_{<p}} - \text{id}_{\mathcal{M}_{<p}})^i \mathcal{M}_{<p} \subset \mathcal{M}_{<p}(i)$.

By Proposition 3.2, $c(n) \equiv \sum_{i \geq 1} c_i n^i \bmod \mathcal{M}(p-1)$, where all $c_i \in \mathcal{M}(i)$. This immediately implies that

$$(\text{id}_{\mathcal{L}} \otimes h_{<p}^n)f \equiv \sum_{i \geq 0} f_i n^i \bmod \mathcal{M}_{<p}(p-1),$$

where $f_0 = f$ and all $f_i \in \mathcal{M}_{<p}(i)$.

Definition. $\bar{\mathcal{M}}^f$ is the minimal Lie subalgebra in $\bar{\mathcal{M}}_{<p}$ containing $\bar{\mathcal{M}}$ and all the elements $(\text{Ad}h_{<p}^n \otimes \text{id}_{\mathcal{K}_{<p}})\bar{f}$ with $n \in \mathbb{N}$.

Note that $\bar{\mathcal{M}}^f$ does not depend on a choice of the lift $h_{<p}$. We can also define $\bar{\mathcal{M}}^f$ as the minimal subalgebra in $\bar{\mathcal{M}}_{<p}$ containing $\bar{\mathcal{M}}$ and all $f^{(i)} \bmod \mathcal{M}_{<p}(p-1)$. Clearly, $\text{id}_{\mathcal{L}} \otimes h_{<p}$ acts on $\bar{\mathcal{M}}^f$ (use that $A \otimes \text{id}_{\mathcal{K}_{<p}}$ and $\text{id}_{\mathcal{L}} \otimes h_{<p}$ commute), this action is completely determined

by the knowledge of $(\text{id}_{\mathcal{L}} \otimes h_{<p})f$, and we can replace $\bar{\mathcal{M}}_{<p}$ by $\bar{\mathcal{M}}^f$ when studying the action of \mathcal{G}_h on \bar{f} .

The filtration $\bar{\mathcal{M}}_{<p}(i)$ induces the filtration $\bar{\mathcal{M}}^f(i)$ on $\bar{\mathcal{M}}^f$, and for all i , $f^{(i)} \bmod \mathcal{M}_{<p}(p-1)$ and $f_i \bmod \mathcal{M}_{<p}(p-1)$ belong to $\bar{\mathcal{M}}^f(i)$.

Now we can apply the results of Subsection 3.2 and introduce the appropriate action $\text{id}_{\mathcal{L}} \otimes h_{<p}^U : \bar{\mathcal{M}}^f \rightarrow \bar{\mathcal{M}}^f \otimes \mathbb{F}_p[[U]]$ of \mathbb{G}_a on $\bar{\mathcal{M}}^f$. This action appears as extension of the action $\text{id}_{\mathcal{L}} \otimes h^U : \bar{\mathcal{M}} \rightarrow \bar{\mathcal{M}} \otimes \mathbb{F}_p[[U]]$ from Subsection 3.1 by setting

$$(\text{id}_{\mathcal{L}} \otimes h_{<p}^U)\bar{f} = \sum_{i \geq 0} f_i \otimes U^i \bmod \mathcal{M}_{<p}(p-1).$$

By Proposition 3.1 the action of $h_{<p}$ is completely determined by the differential $d(\text{id}_{\mathcal{L}} \otimes h_{<p}^U)$.

3.5. Differential $d(\text{id}_{\mathcal{L}} \otimes h_{<p}^U)(\bar{f})$. Using the calculation from Subsection 3.4 we obtain

$$\text{id}_{\mathcal{L}} \otimes h_{<p}^U : \bar{f} \mapsto c(U) \circ f(U) \bmod \mathcal{M}_{<p}(p-1),$$

where $c(U) = \sum_{i \geq 1} c_i U_i$ and $f(U) = f + \sum_{i \geq 1} f^{(i)} U^i$.

It makes sense to introduce the formal operator

$$\text{Ad}h_{<p}^U : \mathcal{L} \rightarrow \mathcal{L} \otimes \mathbb{F}_p[[U]]$$

such that $\text{Ad}h_{<p}^U(l) = \sum_{i \geq 0} l_i U^i$, where $l_i = 0$ if $i \geq p$ and for any $n \in \mathbb{N}$, $\text{Ad}h_{<p}^U|_{U=n} = \text{Ad}h_{<p}^n$. Similarly to Subsection 3.2 for all $i \geq 0$, $l_i = (\text{adh}_{<p})^i l / i!$ and $\text{Ad}(h_{<p}^U) \equiv \text{id}_{\mathcal{L}} + \text{adh}_{<p} U \bmod U^2$. This gives the following formal congruence modulo $\mathcal{M}(p-1) \otimes \mathbb{F}_p[[U]]$:

$$(3.3) \quad (\text{id}_{\mathcal{L}} \otimes h^U)(e) \circ c(U) \equiv ((\sigma c)U) \circ \sum_{a \in \mathbb{Z}^0(p)} t^{-a} (\text{Ad}h_{<p}^U \otimes \text{id}_{\mathcal{K}})(D_{ao}).$$

(Note that $\sigma U = U$.)

Remark. The maps $\text{id}_{\mathcal{L}} \otimes h_{<p}^U$ and $\text{id}_{\mathcal{L}} \otimes h^U$ are defined only on, resp., $\bar{\mathcal{M}}_{<p}^f$ and $\bar{\mathcal{M}}$. However, we shall use the notation $(\text{id}_{\mathcal{L}} \otimes h_{<p}^U)f$ and $(\text{id}_{\mathcal{L}} \otimes h^U)e$ if they appear in congruences modulo, resp., $\mathcal{M}_{<p}(p-1)$ and $\mathcal{M}(p-1)$.

Therefore, we can specify $(\text{id}_{\mathcal{L}} \otimes h_{<p}^U)\bar{f}$ by the following linearization of (3.2). Recall, cf. Subsection 2.1, that $h(t) = t \widetilde{\text{exp}}(\varepsilon^p) \bmod t^{pc_0+1}$, where $\varepsilon^p = \sum_{i \geq 0} A_i(h) t^{c_0+pi}$, all $A_i(h) \in k$ and $A_0(h) \neq 0$. Then by Proposition 2.1, $(\text{id}_{\mathcal{L}} \otimes h^U)(t) = t \widetilde{\text{exp}}(U \varepsilon^p) \bmod t^{pc_0+1}$. Therefore,

$$d(\text{id}_{\mathcal{L}} \otimes h^U)e \equiv - \sum_{a \in \mathbb{Z}^0(p)} t^{-a} \varepsilon^p a D_{ao} \otimes U \bmod \mathcal{M}(p-1).$$

Proposition 3.5. *We have the following recurrent congruence modulo $\mathcal{M}(p-1)$ for c_1 and $V_a = \text{ad } h_{<p}(D_{a0})$, $a \in \mathbb{Z}^0(p)$,*

$$(3.4) \quad \begin{aligned} & \sigma c_1 - c_1 + \sum_{a \in \mathbb{Z}^0(p)} t^{-a} V_a \equiv \\ & - \sum_{k \geq 1} \frac{1}{k!} t^{-(a_1 + \dots + a_k)} \varepsilon^p [\dots [a_1 D_{a_1 0}, D_{a_2 0}], \dots, D_{a_k 0}] \\ & - \sum_{k \geq 2} \frac{1}{k!} t^{-(a_1 + \dots + a_k)} [\dots [V_{a_1}, D_{a_2 0}], \dots, D_{a_k 0}] \\ & - \sum_{k \geq 1} \frac{1}{k!} t^{-(a_1 + \dots + a_k)} [\dots [\sigma c_1, D_{a_1 0}], \dots, D_{a_k 0}] \end{aligned}$$

The indices a_1, \dots, a_k in all above sums run over $\mathbb{Z}^0(p)$.

Proof. The following properties are very well-known from the Campbell-Hausdorff theory. Suppose X and Y are generators of a free Lie $\mathbb{Q}[[U]]$ -algebra. Then

$$\begin{aligned} (UY) \circ X &\equiv X \circ \left(U \sum_{k \geq 0} \frac{1}{k!} [\dots [Y, \underbrace{X, \dots, X}_{k \text{ times}}]] \right), \\ X + UY &\equiv X \circ \left(U \sum_{k \geq 1} \frac{1}{k!} [\dots [Y, \underbrace{X, \dots, X}_{k-1 \text{ times}}]] \right) \pmod{U^2} \end{aligned}$$

For the first formula cf. [14], Ch.II, Section 6.5 or Exercise 1 for Ch.II, Section 6. The second congruence is much more important; it can be extracted from [14], Ch.II, Section 6.5, Prop.5 or Ch.II, Exercise 3 for Section 6.

Using that the coefficients in the above formulas are p -integral in degrees $< p$ we can use them in the context of Lie \mathbb{F}_p -algebras in the following form (where $E_0(x) = (\widetilde{\exp}(x) - 1)/x$):

$$(3.5) \quad (UY) \circ X = X \circ (U \widetilde{\exp}(\text{ad} X)(Y)) \pmod{U^2}$$

$$(3.6) \quad X + UY = X \circ (U E_0(\text{ad} X)(Y)) \pmod{U^2}$$

Remark. a) In above formulas and this paper we use the following notation: $(\text{ad} X)Y = [Y, X]$ and $(\text{Ad} X)Y = (-X) \circ Y \circ X$; this notation is opposite to the notation used in [14];

b) Note the following easy rules: $X \circ (Y + U^2 Z) \equiv X \circ Y \pmod{U^2}$ and $(UX) \circ (UY) \equiv U(X + Y) \pmod{U^2}$.

Then for the left-hand-side (LHS) of (3.3) modulo U^2 we have:

$$\begin{aligned} & (e + d(\text{id}_{\mathcal{L}} \otimes h^U)e + \dots) \circ (c_1 U + \dots) \equiv \\ & e \circ (E_0(\text{ade})(d(\text{id}_{\mathcal{L}} \otimes h^U))) \circ (c_1 U + \dots) \equiv \end{aligned}$$

$$e \circ (E_0(\text{ade})(d(\text{id}_{\mathcal{L}} \otimes h^U)) + c_1 U)$$

Similarly, the RHS of (3.3) modulo U^2 appears in the following form

$$\begin{aligned} ((\sigma c_1)U + \dots) \circ \left(e + U \sum_{a \in \mathbb{Z}^0(p)} t^{-a} V_a + \dots \right) \equiv \\ e \circ \left(U \sum_{a \in \mathbb{Z}^0(p)} E_0(\text{ade})(t^{-a} V_a) + U \widetilde{\text{exp}}(\text{ade})(\sigma c_1) \right) \end{aligned}$$

It remains to cancel by e and equalize the coefficients for U . \square

Note that the number of different solutions $\{c_1, \{V_a \mid a \in \mathbb{Z}^0(p)\}\}$ of (3.4) is $|\mathcal{L}/\mathcal{L}(p)|$. Indeed, we can arrange the recurrent procedure of solving the congruences (3.4) modulo $\mathcal{L}(s)_{\mathcal{K}}$ where $s = 1, \dots, p$. When $s = 1$ we have only the trivial solution. Then each solution modulo $\mathcal{L}(s)_{\mathcal{K}}$ gives a unique extension for all $V_a \bmod \mathcal{L}(s+1)_k$ and $|\mathcal{L}(s)/\mathcal{L}(s+1)|$ different extensions for $c_1 \bmod \mathcal{L}(s+1)_{\mathcal{K}}$.

So, the number of different solutions of congruence (3.4) equals to the number of different lifts $h_{<p}$ of h . This is not surprising because the lift $h_{<p}$ is completely determined by $f_1 U = d(\text{id}_{\mathcal{L}} \otimes h_{<p}^U)f$ and f_1 is uniquely recovered from the knowledge of the appropriate solution $\{c_1, \{V_a \mid a \in \mathbb{Z}^0(p)\}\}$ due to the following proposition.

Recall that for $m \geq 0$,

$$B_m = \sum_{0 \leq v \leq k \leq m} (-1)^v \binom{k}{v} \frac{v^m}{k+1}$$

are the Bernoulli numbers. One of their well-known properties is that

$$x/(1 - \exp(-x)) = \sum_{m \geq 0} B_m (-t)^m / m!.$$

Proposition 3.6. $d(\text{id}_{\mathcal{L}} \otimes h_{<p}^U)f = f_1 \otimes U$, where

$$f_1 = (\text{ad} h_{<p} \otimes \text{id}_{\mathcal{K}_{<p}})f + \sum_{n \geq 0} (-1)^n (B_n / n!) [\dots [c_1, \underbrace{f, \dots, f}_{n \text{ times}}].$$

Proof. In earlier notation we have modulo U^2 (use (3.5) and (3.6)):

$$\begin{aligned} (\text{id}_{\mathcal{L}} \otimes h_{<p}^U) f &\equiv f + f_1 U \equiv (c_1 U) \circ (f + f^{(1)} U) \\ &\equiv (f + f^{(1)} U) \circ (U \widetilde{\text{exp}}(\text{ad} f) c_1) \\ &\equiv f \circ (E_0(\text{ad} f) f^{(1)} U + \widetilde{\text{exp}}(\text{ad} f) c_1 U) \\ &\equiv f + (f^{(1)} + E_0^{-1}(\widetilde{\text{exp}}(\text{ad} f)) c_1) U. \end{aligned}$$

It remains to note that $E_0(x)^{-1} \exp(x) = x/(1 - \exp(-x))$. \square

3.6. Special cases. Recurrent relation (3.4) describes explicitly step by step the action of the lift $h_{<p}$. We can agree, for example, to find at each step the appropriate values of c_1 and V_a by the use of the operators \mathcal{R} and \mathcal{S} from Subsection 2.2. This will specify uniquely the lift $h_{<p}$ together with its action by conjugation on $\mathcal{L}/\mathcal{L}(p)$ and, therefore, will determine the structure of L_h (and of the group \mathcal{G}_h).

Let (as earlier) $\varepsilon^p = \sum_{i \geq 0} A_i(h) t^{c_0 + pi}$, where all $A_i(h) \in k$ and $A_0(h) \neq 0$. Then we obtain modulo $C_2(\mathcal{L}_K) + \mathcal{L}(p)_K$ the following congruence

$$(3.7) \quad \sigma c_1 - c_1 + \sum_{a \in \mathbb{Z}^0(p)} t^{-a} V_a \equiv - \sum_{\substack{a \in \mathbb{Z}^0(p) \\ i \geq 0}} A_i(h) t^{c_0 + pi - a} a D_{a0}.$$

This implies that:

- $(\text{ad } h_{<p})(D_0) \in C_2(\mathcal{L}) + \mathcal{L}(p)$;
- for all $b \in \mathbb{Z}^+(p)$,

$$V_b \equiv - \sum_{i \geq 0} A_i(h) b D_{b+c_0+pi,0} \bmod C_2(\mathcal{L}_k) + \mathcal{L}(p)_k$$

The second relation means that all generators of \mathcal{L}_k of the form D_{an} with $a > c_0$ can be eliminated from the minimal system of generators of L_k (use that $A_0(h) \neq 0$ and, therefore, all $D_{b+c_0,0}$ belong to the ideal of second commutators $C_2(L_{h,k}) = (\text{ad } h_{<p})\mathcal{L}_k + C_2(\mathcal{L}_k) \bmod \mathcal{L}(p)_k$). The first relation then means that L_h has only one relation with respect to any minimal set of generators. This terminology formally makes sense because in the category of Lie \mathbb{F}_p -algebras of nilpotent class $< p$ the algebras of the form $\mathfrak{L}/C_p(\mathfrak{L})$, where \mathfrak{L} is a free Lie \mathbb{F}_p -algebra, play a role of free objects. The same remark also can be used for the category of, say, p -groups of period p and of nilpotent class $< p$. Therefore, \mathcal{G}_h can be treated as an object of this category with finitely many generators and one relation.

As an illustration of Proposition 3.5 we can make the first central step to obtain the following explicit formulas for V_a modulo $\mathcal{L}(3)_k$ (the elements $\mathcal{F}_{\gamma,-N}^0$ are generators of ramification ideals introduced in Subsection 1.4):

$$V_0 \equiv - \sum_{\substack{i \geq 0 \\ 0 \leq n < N_0}} \sigma^n(A_i(h)) \sigma^n(\mathcal{F}_{c_0+pi,0}^0)$$

and for $a \in \mathbb{Z}^+(p)$,

$$V_a \equiv - \sum_{\substack{n \geq 1 \\ i \geq 0}} \sigma^n(A_i(h) \mathcal{F}_{c_0+pi+a/p^n,-n}^0) - \sum_{\substack{m \geq 0 \\ i \geq 0}} \sigma^n(A_i(h) \mathcal{F}_{c_0+pi+ap^m,0}^0).$$

Below we shall study different lifts $h_{<p}$ by introducing a linearization procedure which will allow us (in particular) to replace $\text{Ad } h_{<p}$ by $\text{ad } h_{<p}$.

Remark. a) For any $N \geq 0$, $\mathcal{F}_{c_0+pi,-N}^0 \equiv \mathcal{F}_{c_0+pi,0}^0 \bmod \mathcal{L}(3)_k$ and $\mathcal{F}_{c_0+pi+ap^m,-N}^0 \equiv \mathcal{F}_{c_0+pi+ap^m,0}^0 \bmod \mathcal{L}(3)_k$;

b) for any $N \geq n \geq 1$, $\mathcal{F}_{c_0+pi+a/p^n,-N}^0 \equiv \mathcal{F}_{c_0+pi+a/p^n,-n}^0 \bmod \mathcal{L}(3)_k$;

c) if m is such that $c_0+pi+ap^m > 2(c_0-1)$ then $\mathcal{F}_{c_0+pi+ap^m,0}^0 \in \mathcal{L}(3)_k$;

d) if n is such that $(c_0-1)(1+p^{-n}) < c_0$ then $\mathcal{F}_{c_0+pi+a/p^n,0}^0 \in \mathcal{L}(3)_k$.

Sketch briefly the proof of above formulas for $V_a \bmod \mathcal{L}(3)_k$.

From (3.7) we obtain (apply the operator \mathcal{S} from Subsection 2.2)

$$c_1 \equiv \sum_{\substack{a \in \mathbb{Z}^0(p) \\ i, n \geq 0}} \sigma^n A_i(h) t^{p^n(c_0+pi-a)} a D_{an} \bmod \mathcal{L}(3)_K.$$

Then the right-hand side of (3.4) modulo $\mathcal{L}(3)_K$ appears as

$$\begin{aligned} & - \sum_{a,i} A_i(h) t^{c_0+pi-a} a D_{a0} - \frac{1}{2} \sum_{a_1, a_2, i} A_i(h) t^{c_0+pi-a_1-a_2} a_1 [D_{a_1 0}, D_{a_2 0}] \\ & + \frac{1}{2} \sum_{a_1, a_2, i} A_i(h) t^{-(a_1+a_2)} a_1 [D_{a_1+c_0+pi, 0}, D_{a_2 0}] \\ & - \sum_{\substack{a_1, a_2, n, i \\ 0 < a_1 < c_0+pi}} t^{p^{n+1}(c_0+pi-a_1)-a_2} a_1 [D_{a_1 n_1}, D_{a_2 0}] \end{aligned}$$

In the above sums we have in mind that the indices a, a_1, a_2 run over $\mathbb{Z}^0(p)$, $i, n \geq 1$ and $m \geq 0$. The third sum can be ignored because all $D_{a_1+c_0+pi, 0} \in C_2(L_k)$ and for the similar reason we can ignore the restriction $0 < a_1 < c_0 + pi$ in the last sum. It remains to group the summands with non-negative exponents of t and apply the operator \mathcal{R} .

4. ARITHMETICAL LIFTS

In Section 3 we considered the lifts $h_{<p}$ of $h \in \text{Aut} \mathcal{K}$ to $\mathcal{K}_{<p}$ of \mathcal{K} . All such lifts generate the group $\tilde{\mathcal{G}}_h \subset \text{Aut}(\mathcal{K}_{<p})$. The images of the lifts $h_{<p}$ in $\mathcal{G}_h = \tilde{\mathcal{G}}/\tilde{\mathcal{G}}_h^p C_p(\tilde{\mathcal{G}}_h)$ can be described quite efficiently via their differentials $d(\text{id}_{\mathcal{L}} \otimes h_{<p}^U)$. In this Section we introduce the concept of arithmetical lift $h_{<p}$ and prove that this property depends only on the image of $h_{<p}$ in \mathcal{G}_h and can be characterised in terms related to their differentials $d(\text{id}_{\mathcal{L}} \otimes h_{<p}^U)$.

4.1. Arithmetical lifts. The following brief sketch of the ramification theory of continuous maps of complete discrete valuation fields with perfect residue field is based on the papers [15, 30, 31].

Let E be a complete discrete valuation field with perfect residue field k_E and the maximal ideal \mathfrak{m}_E . Let \hat{E}_{sep} be the completion of a separable closure E_{sep} of E . Denote by v_E the unique extension of the normalized valuation on E to \hat{E}_{sep} . Let \mathcal{I}_E be the group of all continuous automorphisms of \hat{E}_{sep} which are compatible with v_E and induce the identity map on the residue field of E_{sep} . If F is a finite extension of E in E_{sep} then we always assume that $F_{sep} = E_{sep}$ and, therefore, obtain a natural identification $\mathcal{I}_E = \mathcal{I}_F$. Note that the inertia subgroup Γ_E^0 of $\Gamma_E = \text{Gal}(E_{sep}/E)$ is a subgroup in \mathcal{I}_E .

For any $F \subset E_{sep}$ let $\text{Iso}^0(F, \hat{E}_{sep})$ be the set of all continuous field isomorphisms $F \rightarrow \hat{E}_{sep}$ which are compatible with valuations and induce the identity on the residue field of F .

For $g \in \text{Iso}^0(F, \hat{E}_{sep})$, let $v(g) = \min \{v_F(g(a) - a) \mid a \in \mathfrak{m}_F\} - 1$.

For $x \geq 0$, set $\mathcal{I}_{F,x} = \{g \in \text{Iso}^0(F, \hat{E}_{sep}) \mid v(g) \geq x\}$.

Let $\mathcal{I}_{F/E}$ be the subset of all $g \in \text{Iso}^0(F, \hat{E}_{sep})$ which induce the identity map on E and k_F . For $x \geq 0$, let

$$\mathcal{I}_{F/E,x} = \mathcal{I}_{F,x} \bigcap \mathcal{I}_{F/E}.$$

If $\iota_1, \iota_2 \in \mathcal{I}_{F/E}$ and $x \geq 0$ then ι_1 and ι_2 are x -equivalent iff for any $a \in \mathfrak{m}_F$, $v_F(\iota_1(a) - \iota_2(a)) \geq 1 + x$. Denote by $(\mathcal{I}_{F/E} : \mathcal{I}_{F/E,x})$ the number of x -equivalent classes in $\mathcal{I}_{F/E}$. Then the Herbrand function for the field extension F/E can be defined for all $x \geq 0$, as $\varphi_{F/E}(x) = \int_0^x (\mathcal{I}_{F/E} : \mathcal{I}_{F/E,x})^{-1} dx$. This function has the following properties:

- $\varphi_{F/E}$ is a piece-wise linear function with finitely many edges;
- if $L \supset F \supset E$ is a tower of finite field extensions then for any $x \geq 0$, $\varphi_{L/E}(x) = \varphi_{F/E}(\varphi_{L/F}(x))$;
- the last edge point of the graph of $\varphi_{F/E}$ is $(x(F/E), v(F/E))$, where

$$x(F/E) = \inf \{x \geq 0 \mid (\mathcal{I}_{F/E} : \mathcal{I}_{F/E,x}) = |\mathcal{I}_{F/E}|\}$$

is the largest lower and $v(F/E) = \varphi_{F/E}(x(F/E))$ is the largest upper ramification numbers for the extension F/E .

The following proposition is just a direct adjustment of the appropriate fact from the classical ramification theory for finite Galois extensions.

Proposition 4.1. *Suppose $f \in \text{Iso}^0(E, \hat{E}_{sep})$ and $v(f) = x$. Then*

$$\max\{v(g) \mid g \in \text{Iso}^0(F, \hat{E}_{sep}), g|_E = f\} = \varphi_{F/E}(x).$$

Proof. We can assume that F/E is totally ramified of degree d .

Suppose θ is a uniformizing element in F and $P(T) \in E[T]$ is its minimal monic polynomial over E . Then $P(T) = T^d + a_1 T^{d-1} + \dots + a_d$ is an Eisenstein polynomial and $v(f) = v_E(f(a_d) - a_d) - 1 = y$.

Note that for all $1 \leq i < d$, $v_E(f(a_i)\theta^{d-i} - a_i\theta^{d-i}) > v_E(f(a_d) - a_d)$, Therefore, $v_E(f_*P(\theta)) = v_E(f_*(P)(\theta) - P(\theta)) = 1 + y$.

Let $\theta_1, \dots, \theta_d$ be all roots of $f_*P(T)$ in \hat{E}_{sep} . Then all d different lifts g_i of f to F are uniquely determined by the condition $g_i(\theta) = \theta_i$, $i = 1, \dots, d$. Clearly, $v(g_i) = v_F(\theta - \theta_i) - 1$.

Assume that $x = v(g_1)$ is maximal, i.e. $1 + x \geq v_F(\theta - \theta_i)$ for all i . It remains to prove that $y = \varphi_{F/E}(x)$.

Let $A_i := v_F(\theta_i - \theta_1) - 1 \geq 0$. Note $A_1 = +\infty$. Then

$$v_F(f_*P(\theta)) = \sum_{1 \leq i \leq d} v_F(\theta - \theta_i) = \sum_{1 \leq i \leq d} \min\{1 + x, 1 + A_i\} = d + \varphi(x)$$

The function $\varphi(x) = \sum_{1 \leq i \leq d} \min\{x, A_i\}$ is piece-wise linear, $\varphi(0) = 0$ and if x is different from all A_i then

$$\varphi'(x) = |\{A_i \mid A_i > x\}| = |\mathcal{I}_{F/E, x}| = (\mathcal{I}_{F/E} : \mathcal{I}_{F/E, x})^{-1}d = d\varphi'_{F/E}(x).$$

Therefore, $\varphi(x) = d\varphi_{F/E}(x)$ and, finally, $1 + y = v_E(f_*P(\theta)) = d^{-1}v_F(f_*P(\theta)) = d^{-1}(d + d\varphi_{F/E}(x)) = 1 + \varphi_{F/E}(x)$. \square

The ramification filtration $\{\mathcal{I}_E^{(v)}\}_{v \geq 0}$ on \mathcal{I}_E appears as a decreasing sequence of the subsets $\mathcal{I}_E^{(v)}$ of \mathcal{I}_E , which consists of $\iota \in \mathcal{I}_E$ such that for any finite extension F of E , $\iota|_F \in \mathcal{I}_{F, v(F)}$, where $\varphi_{F/E}(v(F)) = v$. Note that $\mathcal{I}_E^{(v)} = \mathcal{I}_F^{(v(F))}$ and $\Gamma_E \cap \mathcal{I}_E^{(v)}$ is the usual higher ramification subgroup $\Gamma_E^{(v)}$ of Γ_E with the upper number v . The largest ramification number $v(F/E)$ is characterized by the following property:

- the ramification subgroup $\Gamma_E^{(v)}$ acts trivially on F iff $v > v(F/E)$.

Definition. Suppose F'/F is a finite extension in E_{sep} , $g \in \text{Iso}^0(F, \hat{E}_{sep})$, $g' \in \text{Iso}^0(F', \hat{E}_{sep})$ is a lift of g , i.e. $g'|_F = g$. Then g' is arithmetical if $v(g) = \varphi_{F'/F}(v(g'))$.

Proposition 4.1 implies the following property.

Proposition 4.2. Suppose $g \in \text{Iso}(F, \hat{E}_{sep})$ and $F \subset F' \subset E_{sep}$. Then:

- g admits an arithmetical lift g' to F' ;
- in the case when F'/F is Galois we have: a lift g'' of g to F' is also arithmetical if and only if $g' \equiv g'' \pmod{\Gamma_F^{(v(g))}}$.

As an application of part b) note the following.

Let $F^{(v(g))}$ be the subfield of E_{sep} fixed by $\Gamma_F^{(v(g))}$. Then:

— a lift g_{sep} of g to E_{sep} is arithmetical (i.e. it is arithmetical when restricted to any finite extension of F in E_{sep}) if and only if $g^{(v(g))} := g_{sep}|_{F^{(v(g))}}$ is arithmetical.

— $g^{(v(g))}$ is a unique arithmetical lift of g to $F^{(v(g))}$.

4.2. Characterization of arithmetical lifts. Suppose $h_{<p}$ is an arithmetical lift of h . Then restriction of $h_{<p}$ to any subfield between \mathcal{K} and $\mathcal{K}_{<p}$ is also arithmetical (use the property of composition of Herbrand functions).

By Proposition 4.2b) such lift $h_{<p}$ is unique modulo the ramification subgroup $\mathcal{G}^{(c_0)} = G(\mathcal{L}^{(c_0)})$. Therefore, we can characterize arithmetical lifts $h_{<p}$ by studying the action of $h_{<p}$ on

$$f \bmod \mathcal{L}_{\mathcal{K}_{<p}}^{(c_0)} \in \mathcal{L}_{\mathcal{K}^{(c_0)}} \bmod \mathcal{L}_{\mathcal{K}_{<p}}^{(c_0)},$$

where $\mathcal{K}^{(c_0)} = \mathcal{K}_{<p}^{G(\mathcal{L}^{(c_0)})}$, cf. Subsection 1.3. The following Proposition provides us with the opportunity to characterize arithmetical lifts by working with $\tilde{f} = f \bmod \mathcal{M}_{<p}(p-1)$.

Proposition 4.3. $\mathcal{L}(p) \subset \mathcal{L}^{(c_0)}$.

Proof. Recall that $\text{wt}(D_{an}) = s$ means that $(s-1)c_0 \leq a < sc_0$. Use explicit formulas for the generators $\mathcal{F}_{\gamma, -N}^0$ of ramification ideals from Subsection 1.4 to prove by induction on $s \geq 1$ that if $\text{wt}(D_{an}) = s$ then $D_{an} \in \mathcal{L}_k^{(c_0)} + C_s(\mathcal{L}_k)$. This implies that if $l \in \mathcal{L}_k$ and $\text{wt}(l) \geq p$ then $l \in C_p(\mathcal{L}_k) \bmod \mathcal{L}_k^{(c_0)}$, but $C_p(\mathcal{L}_k) = 0$. Proposition is proved. \square

So, the property for $h_{<p}$ to be arithmetical can be stated in terms of the differential $(\text{id}_{\mathcal{L}} \otimes h_{<p}^U)f = f_1 \otimes U$ or, equivalently in terms of $(\text{adh}_{<p} \otimes \text{id}_{\mathcal{K}_{<p}})f$ and the linear part $c_1 \in \mathcal{L}_{\mathcal{K}}$ of $c(U)$, cf. Proposition 3.6.

Note that if $h_{<p}$ is arithmetical and for any $g \in \mathcal{G}$, $h_{<p}^{-1}gh_{<p} \equiv g \bmod \mathcal{G}^{(c_0)}$. (Indeed, $g^{-1}h_{<p}g$ is another lift of $h_{<p}$ which is also arithmetical and, therefore, it coincides with $h_{<p}$ modulo $\mathcal{G}^{(c_0)}$.) Therefore, $\text{Ad}h_{<p} \equiv \text{id}_{\mathcal{L}} \bmod \mathcal{L}^{(c_0)}$, or equivalently, $\text{adh}_{<p}(\mathcal{L}) \subset \mathcal{L}^{(c_0)}$. In particular,

$$(\text{Ad}h_{<p} \otimes \text{id}_{\mathcal{K}_{<p}})(f) \equiv f \bmod \mathcal{L}_{\mathcal{K}_{<p}}^{(c_0)}$$

and the property for $h_{<p}$ to be arithmetical can be stated completely in terms of $c_1 \bmod \mathcal{M}(p-1) + \mathcal{L}_{\mathcal{K}}^{(c_0)}$, cf. Subsection 3.5. Even more, we are going to establish this characterization in terms related only to $c_1(0) \in \mathcal{L}_k$, where we set $c_1 = \sum_{m \in \mathbb{Z}} c_1(m)t^m$ with all $c_1(m) \in \mathcal{L}_k$.

Theorem 4.4. *The following properties are equivalent:*

- a) a lift $h_{<p}$ of h is arithmetical;
- b) $\text{adh}_{<p}(\mathcal{L}) \subset \mathcal{L}^{(c_0)}$ and for a sufficiently large N ,

$$c_1 \equiv \sum_{\gamma, j} \sum_{0 \leq i < N} \sigma^i(A_j(h) \mathcal{F}_{\gamma, -i}^0 t^{-\gamma+c_0+pj}) \bmod \mathcal{L}_{\mathcal{K}}^{(c_0)} + \mathcal{M}(p-1);$$

c) for a sufficiently large N ,

$$c_1(0) \equiv \sum_{j \geq 0} \sum_{0 \leq i < N} \sigma^i(A_j(h) \mathcal{F}_{c_0+pj, -i}^0) \bmod \mathcal{L}_k^{(c_0)}.$$

Remark. Note that if $\gamma \geq c_0$ and $i \geq \tilde{N}(c_0)$, cf. Theorem 1.2, then $\mathcal{F}_{\gamma, -i}^0 \in \mathcal{L}_k^{(c_0)}$. There is also $\delta > 0$, cf. Subsection 4.3, such that if $\mathcal{F}_{\gamma, -i}^0 \neq 0$ and $\gamma < c_0$ then $\gamma < c_0 - \delta$. Therefore, in b) we can take $N \geq \max\{\tilde{N}(c_0), \log_p((p-1)c_0/\delta)\}$ and in c) $N \geq \tilde{N}(c_0)$ (use that under these conditions the appropriate RHS's do not depend on N).

4.3. Auxiliary result. We review here a technical result from [3], Section 3. This result was obtained in the contravariant setting. This paper contains explicit calculations with ramification ideals in Lie algebras over \mathbb{Z}/p^{M+1} . It is much easier to follow these calculations when assuming that $M = 0$ (we need only this case). First, introduce the relevant objects and assumptions.

Introducing objects.

Set $M = 0$ (we need the period p case but all constructions in Section 3 of [3] were done modulo p^{M+1}). Let $A = [0, pv_0] \cap \mathbb{Z}^0(p)$, where $v_0 \geq 0$ (later we shall specify $v_0 = c_0$). Let $\mathcal{L}(A)$ be a free Lie algebra over $k \simeq \mathbb{F}_{p^{N_0}}$ with the set of generators

$$\{\mathcal{D}_{an} \mid a \in A^+ = A \cap \mathbb{Z}^+(p), n \in \mathbb{Z}/N_0\} \cup \{\mathcal{D}_0\}$$

For $n \in \mathbb{Z}/N_0$, set $\mathcal{D}_{0n} = (\sigma^n \alpha_0) \mathcal{D}_0$. Consider the σ -linear morphism $\mathcal{L}(A) \rightarrow \mathcal{L}(A)$ such that for all a, n , $\mathcal{D}_{an} \mapsto \mathcal{D}_{a, n+1}$ and denote it also by σ . Then $\mathcal{L}^0 := \mathcal{L}(A)|_{\sigma=\text{id}}$ is a free Lie algebra over \mathbb{F}_p and $\mathcal{L}_k^0 = \mathcal{L}(A)$.

Consider the contravariant analogue of the elements $\mathcal{F}_{\gamma, -N}^0$ from Subsection 1.4 (use the same conditions for all involved indices)

$$\mathcal{F}_{\gamma, -N} = \sum_{1 \leq s < p} (-1)^{s-1} \sum_{\substack{a_1, \dots, a_s \\ n_1, \dots, n_s}} a_1 [\dots [\mathcal{D}_{a_1 \bar{n}_1}, \mathcal{D}_{a_2 \bar{n}_2}], \dots, \mathcal{D}_{a_s \bar{n}_s}]$$

Denote by $\mathcal{L}_N^0(v_0)$ the minimal ideal in \mathcal{L}^0 such that $\mathcal{L}_N^0(v_0)_k$ contains all $\mathcal{F}_{\gamma, -N}$ with $\gamma \geq v_0$. Let $\tilde{N}(v_0, A)$ be such that the ideals $\mathcal{L}_N^0(v_0)$ coincide for all $N \geq \tilde{N}(v_0, A)$ and denote this ideal by $\mathcal{L}^0(v_0)$.

Let $\Gamma = \Gamma(A, v_0)$ be the set of all $\gamma = a_1 p^{n_1} + \dots + a_s p^{n_s}$, where all $a_i \in A$, $0 = n_1 \geq n_2 \geq \dots \geq n_s$, $1 \leq s < p$.

Choosing parameters δ, r^, N^* :*

- a) let $\delta = \delta(A, v_0) > 0$ be sufficiently small such that $v_0 - \delta > \max\{\gamma \mid \gamma \in \Gamma, \gamma < v_0\}$, $p\delta < 2v_0$ and $v_0 - \delta \in \mathbb{Z}[1/p]$;
- b) let r^* be such that $v_p(r^*) = 0$ and $v_0 - \delta < r^* < v_0$;
- c) let $N^* \in \mathbb{N}$ be such that $N^* \geq \tilde{N}(v_0, A) + 1$ and for $q = p^{N^*}$, we have $r^*(q-1) = b^* \in \mathbb{N}$ (note $v_p(b^*) = 0$), $a^* = q(v_0 - \delta) \in p\mathbb{N}$;

d) note that if q satisfies the conditions from c) then any its power q^A with $A \in \mathbb{N}$ also satisfies these conditions; therefore, we can enlarge (if necessary) q to obtain the following inequalities:

$$r^* - (v_0 - \delta) > \frac{r^* + p(v_0 - \delta)}{q}, \quad v_0 - r^* > \frac{-r^* + \varphi^{(c_0)}(e^{(c_0)} c_0(p-1))}{q}$$

All above constructions and choices were made in Subsection 3.1 of [3], except the additional conditions $p\delta < 2v_0$ and the second inequality in d). In this inequality $\varphi^{(c_0)}$ and $e^{(c_0)}$ are the Herbrand function and, resp., the ramification index of the extension $\mathcal{K}^{(c_0)}/\mathcal{K}$. (Here $K^{(c_0)}$ is a subfield of $\mathcal{K}_{<p}$, fixed by $\mathcal{G}^{(c_0)}$; note that $[\mathcal{K}^{(c_0)} : \mathcal{K}] < \infty$.)

We need also the following auxiliary field extension $\mathcal{K}' = \mathcal{K}(r^*, N^*)$ of \mathcal{K} such that:

- $[\mathcal{K}' : \mathcal{K}] = q$;
- the Herbrand function $\varphi_{\mathcal{K}'/\mathcal{K}}$ has only one edge point at (r^*, r^*) ;
- $\mathcal{K}' = k((t'))$, where $t = t'^q E(t'^{b^*})^{-1}$ with the Artin-Hasse exponential $E(X) = \exp(X + X^p/p + \dots + X^{p^n}/p^n + \dots)$.

The field \mathcal{K}' played very important role in our approach to the ramification filtration in [1, 2, 3, 8, 9, 11]. Note that \mathcal{K}'/\mathcal{K} is not a p -extension if $N^* > 1$.

Specifying the notation from [3] to our situation set $\hat{N} = \tilde{N} = N^* - 1$ (in particular, \tilde{N} could be different from $\tilde{N}(v_0, A)$ introduced earlier).

Let $\hat{e}_{\mathcal{L}}^{(0)} = \sum_{a \in \mathbb{Z}^0(p)} t^{-a} \mathcal{D}_{a0}$ and $e'_{\mathcal{L}}{}^{(q)} = \sum_{a \in \mathbb{Z}^0(p)} t'^{-aq} \mathcal{D}_{a0}$. (We follow maximally close the notation from [3].) Clearly, the elements $\hat{e}_{\mathcal{L}}^{(0)}$ and $e'_{\mathcal{L}} := \sum_{a \in \mathbb{Z}^0(p)} t'^{-a} \mathcal{D}_{a, -N^*}$ are analogs of our element e introduced in Subsection 1.3 and $\sigma^{N^*} e'_{\mathcal{L}} = e'_{\mathcal{L}}{}^{(q)}$.

Then we have the elements $E_0 = \widetilde{\exp}(e_{\mathcal{L}}^{(0)})$, $E'_0 = \sigma^{N^*} \widetilde{\exp}(e'_{\mathcal{L}})$ and (where we specify $m = 1$) the element $\Phi_0^{(\tilde{N})} = \Phi_{01}^{(\tilde{N})} = \Phi_{11} \Phi_{21}$, cf. the first paragraph on p.890 in the proof of Lemma 2 of Subsection 3.10. Explicit expressions for Φ_{11} and Φ_{21} from the second paragraph on p.890 should look slightly corrected as follows

$$\Phi_{11} = \widetilde{\exp}(e'_{\mathcal{L}}{}^{(q)}) \widetilde{\exp}(\sigma e'_{\mathcal{L}}{}^{(q)}) \dots \widetilde{\exp}(\sigma^{\tilde{N}} e'_{\mathcal{L}}{}^{(q)})$$

$$\Phi_{21} = \widetilde{\exp}(-\sigma^{\tilde{N}} e_{\mathcal{L}}^{(0)}) \dots \widetilde{\exp}(-\sigma e_{\mathcal{L}}^{(0)}) \widetilde{\exp}(-e_{\mathcal{L}}^{(0)}).$$

As a result, $\Phi_0^{(\tilde{N})} = \widetilde{\exp}(\phi_0^{(\tilde{N})})$, where $\phi_0^{(\tilde{N})} \in G(\mathcal{L}_{\mathcal{K}'}^0)$ is equal to

$$\phi_0^{(\tilde{N})} = e'_{\mathcal{L}}{}^{(q)} \circ (\sigma e'_{\mathcal{L}}{}^{(q)}) \circ \dots \circ (\sigma^{\tilde{N}} e'_{\mathcal{L}}{}^{(q)}) \circ (-\sigma^{\tilde{N}} \hat{e}_{\mathcal{L}}^{(0)}) \circ \dots \circ (-\sigma \hat{e}_{\mathcal{L}}^{(0)}) \circ (-\hat{e}_{\mathcal{L}}^{(0)})$$

Suppose $O = O_{\mathcal{K}'}$ is the valuation ring of \mathcal{K}' . Then the properties of $\Phi_0^{(\tilde{N})}$ from Proposition 9 of 3.9 a,b) imply (cf. Proposition from Subsection 3.10 of [3]) the following proposition.

Proposition 4.5. a) $\phi_0^{(\tilde{N})}, \sigma\phi_0^{(\tilde{N})} \in \mathcal{L}^0(v_0)_{\mathcal{K}'} + \sum_{1 \leq j < p} t'^{-ja^*} C_j(\mathcal{L}_O^0);$

b) $\phi_0^{(\tilde{N})} \circ \hat{e}_{\mathcal{L}}^0 \equiv e'_{\mathcal{L}} \circ \sigma\phi_0^{(\tilde{N})} \pmod{\mathcal{L}\mathcal{H}_1^0}$, where

$$\mathcal{L}\mathcal{H}_1^0 = \mathcal{L}^0(v_0)_{\mathcal{K}'} + t'^{q(b^*-a^*)} \sum_{1 \leq j < p} t'^{-(j-1)a^*} C_j(\mathcal{L}_O).$$

Translate this result into the covariant setting and our notation.

Let $v_0 = c_0$.

Consider the map Π from \mathcal{L}^0 to \mathcal{L} such that $(\Pi \otimes k)(\mathcal{D}_{an}) = D_{an}$ for all $a \in A$ and $n \in \mathbb{Z}/N_0$ and for any $l_1, l_2 \in \mathcal{L}^0$, $\Pi([l_1, l_2]) = [\Pi(l_2), \Pi(l_1)]$.

Then the (ramification) ideal $\mathcal{L}^0(c_0)$ is mapped to $\mathcal{L}^{(c_0)}$. Essentially, Π is a morphism of Lie algebras (where \mathcal{L}^0 is taken with the opposite Lie structure) and it induces isomorphism of the appropriate quotients by $\mathcal{L}^0(c_0)$ and $\mathcal{L}^{(c_0)}$, respectively (use that all $D_{an} \in \mathcal{L}_k^{(c_0)}$ if $a > pc_0$).

Clearly, $\Pi(\hat{e}_{\mathcal{L}}^{(0)}) = e$ and $\Pi(e'_{\mathcal{L}}) \equiv e' := \sum_{a \in \mathbb{Z}^0(p)} t'^{-a} D_{a, -N^*} \pmod{\mathcal{L}_{\mathcal{K}'}^{(c_0)}}$.

Therefore, we have $\Pi(\phi_0^{(\tilde{N})}) := \phi_0 = (-\phi) \circ (\sigma^{N^*} \phi')$, where we set $\phi = (\sigma^{\tilde{N}} e) \circ \dots \circ (\sigma e) \circ e$ and $\phi' = (\sigma^{\tilde{N}} e') \circ \dots \circ (\sigma e') \circ e'$.

Let

$$\mathcal{M}_{\mathcal{K}'} := \sum_{1 \leq j < p} t'^{-c_0 j} \mathcal{L}(j)_{\mathfrak{m}'} + \mathcal{L}(p)_{\mathcal{K}'},$$

where \mathfrak{m}' is the maximal ideal of the valuation ring of \mathcal{K}' . Similarly, set

$$\mathcal{M}_{\mathcal{K}'_{<p}} = \sum_{1 \leq s < p} t'^{-c_0 s} \mathcal{L}(s)_{\mathfrak{m}'_{<p}} + \mathcal{L}(p)_{\mathcal{K}'_{<p}}$$

where $\mathcal{K}'_{<p}$ and $\mathfrak{m}'_{<p}$ are the analogs of $\mathcal{K}_{<p}$ and $\mathfrak{m}_{<p}$ for \mathcal{K}' .

Note that the above introduced modules $\mathcal{M}_{\mathcal{K}'}$ and $\mathcal{M}_{\mathcal{K}'_{<p}}$ are not obtained from \mathcal{M} and, resp., $\mathcal{M}_{<p}$ when we replace \mathcal{K} by \mathcal{K}' . Under such replacement we shall obtain from \mathcal{M} and $\mathcal{M}_{<p}$ the following modules

$$\mathcal{M}' := \sum_{1 \leq j < p} t'^{-c_0 j} \mathcal{L}(j)_{\mathfrak{m}_{\mathcal{K}'}} + \mathcal{L}(p)_{\mathcal{K}'},$$

$$\mathcal{M}'_{<p} := \sum_{1 \leq s < p} t'^{-c_0 s} \mathcal{L}(s)_{\mathfrak{m}'_{<p}} + \mathcal{L}(p)_{\mathcal{K}'_{<p}}.$$

However, note that $\sigma^{N^*} \mathcal{M}' \subset \mathcal{M}_{\mathcal{K}'}$ and $\sigma^{N^*} \mathcal{M}'_{<p} \subset \mathcal{M}_{\mathcal{K}'_{<p}}$.

Proposition 4.6. a) $\phi_0, \sigma(\phi_0) \in \mathcal{M}_{\mathcal{K}'} + \mathcal{L}_{\mathcal{K}'}^{(c_0)}$;

b) $e \circ \phi_0 \equiv (\sigma\phi_0) \circ (\sigma^{N^*} e') \pmod{(t^{c_0(p-1)} \mathcal{M}_{\mathcal{K}'} + \mathcal{L}_{\mathcal{K}'}^{(c_0)})}$

Proof. a) From the definition of a^* it follows that $a^* = (c_0 - \delta)q < c_0 q$. Therefore, for $1 \leq j < p$,

$$t'^{-ja^*} O_{\mathcal{K}'} C_j(\mathcal{L}) \subset t'^{-jc_0} \mathfrak{m}' C_j(\mathcal{L}) \subset t'^{-jc_0} \mathcal{L}(j)_{\mathfrak{m}'}.$$

For part b), we need for $1 \leq j < p$,

$$q(b^* - a^*) - (j - 1)a^* > (p - j - 1)qc_0.$$

This can be rewritten as $q(r^* - (c_0 - \delta)) > r^* + (p - 2)c_0$. This follows from the inequality $p\delta < 2v_0$ in a) and the first inequality in d) from the beginning of this subsection. \square

4.4. Implication a) \Rightarrow b), I. Suppose $h_{<p}$ is arithmetical. We must prove that (cf. discussion in Subsection 4.2)

$$(\text{id}_{\mathcal{L}} \otimes h_{<p}^U)(f) \equiv (c_1 U) \circ f \bmod (U^2 \mathcal{M}_{<p} + U t^{c_0(p-1)} \mathcal{M}_{<p} + U \mathcal{L}_{\mathcal{K}_{<p}}^{(c_0)}),$$

where c_1 is given in the statement of our theorem.

Consider the field \mathcal{K}' from Subsection 4.4. This field is isomorphic to \mathcal{K} and this isomorphism can be extended to an isomorphism of $\mathcal{K}_{<p}$ and its analog $\mathcal{K}'_{<p}$. Let $f' \in \mathcal{M}'_{<p}$ be such that $\sigma f' = e' \circ f'$. Then Proposition 4.6 b) implies the following lemma.

Lemma 4.7. *f' can be chosen in such a way that*

$$f \equiv \phi_0 \circ \sigma^{N^*} f' \bmod \left(t^{c_0(p-1)} \mathcal{M}_{\mathcal{K}'_{<p}} + \mathcal{L}_{\mathcal{K}'_{<p}}^{(c_0)} \right).$$

Proof. Let $g = (-f) \circ \phi_0 \circ \sigma^{N^*} f' \in \mathcal{M}'_{\mathcal{K}'_{<p}}$. Then Proposition 4.6 b) means that $\sigma g \equiv g \bmod (t^{c_0(p-1)} \mathcal{M}_{\mathcal{K}'_{<p}} + \mathcal{L}_{\mathcal{K}'_{<p}}^{(c_0)})$. This congruence implies that $g \in \mathcal{L} + t^{c_0(p-1)} \mathcal{M}_{\mathcal{K}'_{<p}} + \mathcal{L}_{\mathcal{K}'_{<p}}^{(c_0)}$. (Use that $t^{c_0(p-1)} \mathcal{M}_{\mathcal{K}'_{<p}} \subset \mathfrak{m}' \mathcal{L}_{\mathcal{K}'_{<p}}$.) Therefore, we can shift f' by a suitable element of l to obtain that $g \in t^{c_0(p-1)} \mathcal{M}_{\mathcal{K}'_{<p}} + \mathcal{L}_{\mathcal{K}'_{<p}}^{(c_0)}$. The lemma is proved. \square

Now note that $\mathcal{K} \subset \mathcal{K}'$ induces the embeddings $\mathcal{K}_{<p} \subset \mathcal{K}' \mathcal{K}_{<p} \subset \mathcal{K}'_{<p}$. Choose an arithmetical lift (use notation from Subsection 4.1) $h'_{<p} \in \text{Iso}^0(\mathcal{K}'_{<p}, \hat{\mathcal{K}}_{sep})$ of h . (Note that it is not obvious that we can find h' in $\text{Aut}(\mathcal{K}'_{<p})$.) Then the restrictions $h' := h'_{<p}|_{\mathcal{K}'}$ and $h_{<p} := h'_{<p}|_{\mathcal{K}_{<p}}$ are also arithmetical, and we can study $(\text{id}_{\mathcal{L}} \otimes h_{<p})f$ via the following congruence modulo $t^{c_0(p-1)} \mathcal{M}_{\mathcal{K}'_{<p}} + \mathcal{L}_{\mathcal{K}'_{<p}}^{(c_0)}$

$$(\text{id}_{\mathcal{L}} \otimes h_{<p})f \equiv (-\text{id}_{\mathcal{L}} \otimes h)\phi \circ (\text{id}_{\mathcal{L}} \otimes h')\sigma^{N^*} \phi' \circ (\text{id}_{\mathcal{L}} \otimes h'_{<p})\sigma^{N^*} f'.$$

(Recall, $\phi_0 = (-\phi) \circ (\sigma^{N^*} \phi')$, cf. Subsection 4.3.)

Proposition 4.8. $(\text{id}_{\mathcal{L}} \otimes h'_{<p})f' \equiv f' \bmod \left(t^{c_0(p-1)} \mathcal{M}_{\mathcal{K}'_{<p}} + \mathcal{L}_{\mathcal{K}'_{<p}}^{(c_0)} \right).$

Proof. Let $\mathcal{K}'_{<p}^{(c_0)}$ be the subfield of $\mathcal{K}'_{<p}$ fixed by the ramification subgroup $\text{Gal}(\mathcal{K}'_{<p}/\mathcal{K}')^{(c_0)}$. Clearly, the extensions $\mathcal{K}^{(c_0)}/\mathcal{K}$ and $\mathcal{K}'^{(c_0)}/\mathcal{K}'$ are isomorphic and, therefore, $\varphi^{(c_0)}$ and $e^{(c_0)}$ (cf. Subsection 4.3) appear also as the Herbrand function and the ramification index for $\mathcal{K}'^{(c_0)}/\mathcal{K}'$.

Let $h'^{(c_0)}$ be the restriction of $h'_{<p}$ to $\mathcal{K}'_{<p}^{(c_0)}$. Then

$$v(h') = \varphi_{\mathcal{K}'/\mathcal{K}}^{-1}(c_0) = r^* + q(c_0 - r^*)$$

and

$$v(h'^{(c_0)}) = (\varphi^{(c_0)})^{-1}(r^* + q(c_0 - r^*)) > e^{(c_0)} c_0 (p - 1)$$

(use the second inequality from Subsection 4.3 d)). Therefore,

$$(\text{id}_{\mathcal{L}} \otimes h'^{(c_0)} - \text{id}_{\mathcal{M}'_{<p}}) \left(\mathcal{M}'_{<p} \cap \mathcal{L}_{\mathcal{K}'_{<p}(c_0)} \right) \subset t'^{c_0(p-1)} \mathcal{M}'_{<p} \cap \mathcal{L}_{\mathcal{K}'_{<p}(c_0)}.$$

On the other hand, $f' \in \mathcal{M}'_{<p} \cap \mathcal{L}_{\mathcal{K}'_{<p}(c_0)} + \mathcal{L}_{\mathcal{K}'_{<p}(c_0)}$, cf. Subsection 1.3. Therefore, $h'_{<p}(f') \equiv f' \pmod{t'^{c_0(p-1)} \mathcal{M}'_{<p} + \mathcal{L}_{\mathcal{K}'_{<p}(c_0)}}$. The proposition is proved. \square

4.5. **Implication a) \Rightarrow b), II.** Recall that

$$\phi = (\sigma^{\tilde{N}} e) \circ \dots \circ (\sigma e) \circ e, \quad \phi' = (\sigma^{\tilde{N}} e') \circ \dots \circ (\sigma e') \circ e'.$$

Apply identities (3.5) and (3.6) from Subsection 3.2, use the definition of the elements $\mathcal{F}_{\gamma, -N}^0 \in \mathcal{L}_k$ from Subsection 1.4 and use the abbreviation $d_h := d(\text{id}_{\mathcal{L}} \otimes h^U)$:

$$\begin{aligned} e + d_h e &\equiv e \circ \left(\sum_{k \geq 1} (1/k!) [\dots [d_h e, \underbrace{e, \dots, e}_{k-1 \text{ times}}] \dots] \right) \\ &\equiv e \circ \left(-U \sum_{\gamma > 0, j \geq 0} A_j(h) \mathcal{F}_{\gamma, 0}^0 t^{-\gamma + c_0 + pj} \right) \end{aligned}$$

Similarly,

$$\sigma e + \sigma d_h e \equiv \sigma e \circ \left(\sum_{k \geq 1} (1/k!) [\dots [\sigma d_h e, \underbrace{\sigma e, \dots, \sigma e}_{k-1 \text{ times}}] \dots] \right)$$

and then

$$\begin{aligned} &(\sigma e + \sigma d_h e) \circ (e + d_h e) \equiv \\ &(\sigma e) \circ e \circ \left(\sum_{\substack{k_0 \geq 1 \\ k_1 \geq 0}} \frac{1}{k_0! k_1!} [\dots [\sigma d_h e, \underbrace{\sigma e, \dots, \sigma e}_{k_0-1 \text{ times}}], \underbrace{e, \dots, e}_{k_1 \text{ times}}] \dots] \right) \\ &= (\sigma e) \circ e \circ \left(-U \sum_{\substack{\gamma > 0 \\ j \geq 0}} \sum_{0 \leq i \leq 1} \sigma^i(A_j(h) \mathcal{F}_{\gamma, -i}^0 t^{-\gamma + c_0 + pj}) \right) \end{aligned}$$

We can continue similarly to obtain that

$$(\text{id} \otimes h^U) \phi \equiv \phi \circ \left(-U \sum_{\substack{\gamma > 0 \\ j \geq 0}} \sum_{0 \leq i \leq \tilde{N}} \sigma^i(A_j(h) \mathcal{F}_{\gamma, -i}^0 t^{-\gamma + c_0 + pj}) \right) \pmod{U^2}$$

As for the action of h' on ϕ' note that

$$v(h') = r^* + q(c_0 - r^*) > c_0(p-1)$$

(we use that $\varphi^{(c_0)}(e^{(c_0)}x) \geq x$ for any $x \geq 0$).

Therefore, $(\text{id}_{\mathcal{L}} \otimes h')e' \equiv e' \bmod t^{c_0(p-1)}\mathcal{M}'$, $(\text{id}_{\mathcal{L}} \otimes h')(\sigma^{N^*}e') \equiv \sigma^{N^*}e' \bmod t^{c_0(p-1)}\mathcal{M}_{\mathcal{K}'}$ and $(\text{id}_{\mathcal{L}} \otimes h')\phi' \equiv \phi' \bmod t^{c_0(p-1)}\mathcal{M}_{\mathcal{K}'}$.

Finally, we found all three ingredients of $(\text{id}_{\mathcal{L}} \otimes h_{<p})f$ and multiplying them we obtain the congruence for c_1 from b) of our theorem.

4.6. The end of proof of Theorem 4.4. Suppose $h_{<p}$ satisfies b). Then its ingredients c_1 and V_a coincide modulo, resp., $\mathcal{L}_{\mathcal{K}}^{(c_0)}$ and $\mathcal{L}_k^{(c_0)}$ with the similar ingredients of some arithmetical lift of h . Therefore, $h_{<p}$ is arithmetical (because it is arithmetical modulo $\mathcal{L}^{(c_0)}$). This proves that b) \Rightarrow a).

Obviously, b) implies c).

Suppose $h_{<p}$ satisfies c) and its ingredients are c_1 and $\{V_a \mid a \in \mathbb{Z}^0(p)\}$. Choose the maximal $1 \leq s_0 \leq p$ such that $h_{<p} \bmod \mathcal{L}(s_0)$ is arithmetical. We must prove that $s_0 = p$.

Suppose $s_0 < p$.

Let $h_{<p}^0$ be some arithmetical lift of h with the appropriate ingredients c_1^0 and $\{V_a^0 \mid a \in \mathbb{Z}^0(p)\}$. Therefore, $c_1 \equiv c_1^0 \bmod \mathcal{L}_{\mathcal{K}}^{(c_0)} + \mathcal{L}(s_0)_{\mathcal{K}}$. Note that for all $a \in \mathbb{Z}^0(p)$, $V_a \in \mathcal{L}_k^{(c_0)} + \mathcal{L}(s_0)_k$ and $V_a^0 \in \mathcal{L}_k^{(c_0)}$. Then recurrent relation (3.4) (considered at the s_0 -th step) implies that

$$\sigma c_1 - c_1 + \sum_{a \in \mathbb{Z}^0(p)} t^{-a} V_a \equiv \sigma c_1^0 - c_1^0 \bmod \mathcal{L}_{\mathcal{K}}^{(c_0)} + \mathcal{L}(s_0 + 1)_{\mathcal{K}}$$

Therefore, all $V_a \in \mathcal{L}_{\mathcal{K}}^{(c_0)} + \mathcal{L}(s_0 + 1)_{\mathcal{K}}$ and

$$c_1 - c_1^0 \equiv c_1(0) - c_1^0(0) \bmod \mathcal{L}_{\mathcal{K}}^{(c_0)} + \mathcal{L}(s_0 + 1)_{\mathcal{K}}.$$

So, if $c_1(0)$ satisfies c) then $h_{<p}$ is arithmetical modulo $\mathcal{L}(s_0 + 1)_{\mathcal{K}}$. The contradiction. Theorem 4.4 is completely proved.

5. EXPLICIT CALCULATIONS IN L_h

In this Section we apply the above techniques to study $h_{<p}$ modulo $\mathcal{L}(p)$. In Subsection 4 we've just studied the properties of $h_{<p}$ modulo $\mathcal{L}^{(c_0)}$ what was sufficient to characterize the property of $h_{<p}$ to be arithmetical. If we want to describe completely the structure of the Lie algebra L_h we need to know the structure of $h_{<p}$ modulo $\mathcal{L}(p)$.

Suppose $h_{<p}$ is given, as earlier, via

$$(\text{id}_{\mathcal{L}} \otimes h_{<p})f = c \circ (\text{Ad } h_{<p} \otimes \text{id}_{\mathcal{K}_{<p}})f$$

with the appropriate $c \in \mathcal{L}_{\mathcal{K}}$. Then the relevant elements $c_1 \otimes U$ and $V_a = \text{ad } h_{<p}(D_{a0})$, $a \in \mathbb{Z}^0(p)$, satisfy recurrent relation (3.4). This allows us to proceed from solutions $(c_1, \sum_a t^{-a} V_a)$ obtained modulo $\mathcal{M}(p-1) + \mathcal{L}(s)_{\mathcal{K}}$ to the appropriate “more precise” solutions modulo $\mathcal{M}(p-1) + \mathcal{L}(s+1)_{\mathcal{K}}$, for all $1 \leq s < p$.

As earlier, let $c_1 = \sum_{m \in \mathbb{Z}} c_1(m)t^m$, where all $c_1(m) \in \mathcal{L}_k$. Introduce $c_1^+ = \sum_{m > 0} c_1(m)t^m$ and $c_1^- = \sum_{m < 0} c_1(m)t^m$. Then

$$c_1 = c_1^- + c_1(0) + c_1^+.$$

In this Section we find “precise” formulas for c^+ , $c(0)$ and $\text{ad}h_{<p}(D_0)$. When choosing c_1^+ we use the operator \mathcal{S} from Subsection 2.2. When choosing $c_1(0)$ we must act more carefully. The expression for $\text{ad}D_0$ is given in Proposition 5.4 below.

It would be very interesting to resolve completely recurrent relation (3.4) and to find reasonably compact formulas for c_1^- and all the elements $V_a = \text{ad}h_{<p}(D_{a0})$, $a \in \mathbb{Z}^+(p)$. This would generalize explicit calculations from Subsection 3.6. Some steps in this direction were made recently by K.McCabe (Durham University) in his forthcoming Thesis.

5.1. Specifying c_1^+ . Relation (3.4) implies that modulo $\mathcal{M}(p-1)$

$$(5.1) \quad \begin{aligned} & \sigma c_1^+ - c_1^+ \equiv \\ & - \sum_{\substack{k \geq 1 \\ j \geq 0}} \frac{1}{k!} A_j(h) \sum_{a_1, \dots, a_k} t^{c_0 + pj - (a_1 + \dots + a_k)} [\dots [a_1 D_{a_1 0}, D_{a_2 0}], \dots, D_{a_k 0}] \\ & - \sum_{m, k \geq 1} \frac{1}{k!} \sum_{a_1, \dots, a_k} t^{pm - (a_1 + \dots + a_k)} [\dots [\sigma c_1(m), D_{a_1 0}], \dots, D_{a_k 0}]. \end{aligned}$$

In both above sums the indices a_1, \dots, a_k run over $\mathbb{Z}^0(p)$ with the restrictions $a_1 + \dots + a_k < c_0 + pj$ for the first sum and $a_1 + \dots + a_k < pm$ for the second sum.

Note that $c_1^+ \bmod \mathcal{M}(p-1)$ is defined uniquely by (5.1). Of course, it is obtained by applying the operator \mathcal{S} from Subsection 2.2 to the RHS of the above congruence.

Definition. For $n^* \geq n_*$, denote by $\mathcal{F}_{\gamma, [n^*, n_*]}^0$ the partial sum of $\sigma^{n^*} \mathcal{F}_{\gamma, -N^*}^0$ containing only the terms with $[\dots [D_{a_1 \bar{n}_1}, D_{a_2 \bar{n}_2}], \dots, D_{a_s \bar{n}_s}]$, where $n_1 = n^*$ and $n_s = n_*$. In other words, we keep only the terms such that $n^* = \max\{n_i \mid 1 \leq i \leq s\}$ and $n_* = \min\{n_i \mid 1 \leq i \leq s\}$.

Proposition 5.1. *Let $N^* \in \mathbb{N}$ be the natural number chosen in Subsection 4.3. Then*

$$c_1^+ \equiv \sum_{\substack{j \geq 0 \\ 0 \leq n < N^*}} \sum_{\gamma < c_0 + pj} \sigma^n(A_j(h) \mathcal{F}_{\gamma, -n}^0) t^{p^n(c_0 + pj - \gamma)} \bmod \mathcal{M}(p-1).$$

Remark. Instead of N^* we can take any $N \in \mathbb{N}$ such that $N \geq \log_p(c_0(p-1)/\delta)$, cf. the remark after the statement of Theorem 4.4.

Proof of Proposition. Prove proposition by establishing the formula for c_1^+ modulo $\mathcal{M}(p-1) + C_s(\mathcal{L}_K)$ by induction on $1 \leq s \leq p$.

If $s = 1$ there is nothing to prove.

Suppose $s < p$ and Proposition is proved modulo $\mathcal{M}(p-1) + C_s(\mathcal{L}_K)$. Prove that modulo $\mathcal{M}(p-1) + C_{s+1}(\mathcal{L}_K)$

$$(5.2) \quad \sigma c_1^+ - c_1^+ \equiv \sum_{\substack{j \geq 0 \\ 0 \leq n < N^*}} \sigma^n(A_j(h)) \sum_{\gamma < c_0 + pj} \mathcal{F}_{\gamma, [n, 0]}^0 t^{p^n(c_0 + pj - \gamma)}.$$

Note that for $n = 0$,

$$\mathcal{F}_{\gamma, [0, 0]}^0 = \sum_{a_1, \dots, a_k} \frac{1}{k!} [\dots [a_1 D_{a_1 0}, D_{a_2 0}], \dots, D_{a_k 0}]$$

and for $n > 0$,

$$\mathcal{F}_{\gamma, [n, 0]}^0 = \sum_{\substack{k \geq 1, \gamma' > 0 \\ a_1, \dots, a_k}} \frac{1}{k!} [\dots [\sigma^n \mathcal{F}_{\gamma', -(n-1)}^0, D_{a_1 0}], \dots, D_{a_k 0}].$$

In both sums the indices a_1, \dots, a_k run over $\mathbb{Z}^0(p)$ with the restrictions $a_1 + \dots + a_k = \gamma$ in the first case and $p^n \gamma' + a_1 + \dots + a_k = \gamma$ in the second case.

The first formula allows us to identify the first line of the RHS in (5.1) with the part of (5.2) which corresponds to $n = 0$. The second formula allows us to rewrite modulo $C_{s+1}(\mathcal{L}_K)$ the second line of the RHS in (5.1) (under inductive assumption) as the part of a) which corresponds to $n > 0$.

Let Ω be the right-hand side of (5.2). Applying \mathcal{S} we obtain $c_1^+ = \sum_{m \geq 0} \sigma^m \Omega$ and, therefore, modulo $\mathcal{M}(p-1) + C_{s+1}(\mathcal{L}_K)$ we have:

$$c_1^+ \equiv - \sum_{n, m, j} \sigma^{n+m} (A_j(h) \mathcal{F}_{\gamma, [0, -n]}^0) t^{p^{n+m}(c_0 + pj - \gamma)}.$$

Modulo $\mathcal{M}(p-1)$ we can assume that $n_1 = n + m < N^*$ (use remark after statement of Theorem 4.4) and rewrite the above RHS as

$$\sum_{\gamma, j, n_1} \sigma^{n_1} \left(A_j(h) \sum_{0 \leq m \leq n_1} \mathcal{F}_{\gamma, [0, -m]}^0 \right) t^{p^{n_1}(c_0 + pj - \gamma)}.$$

It remains to note that $\sum_{0 \leq m \leq n_1} \mathcal{F}_{\gamma, [0, -m]}^0 = \mathcal{F}_{\gamma, -n_1}^0$.

The proposition is proved. \square

5.2. Specifying $c_1(0)$. By (3.4) we have modulo $\mathcal{L}(p)_k$

$$(5.3) \quad \begin{aligned} \sigma c_1(0) - c_1(0) + V_0 \equiv & \\ & - \sum_{\substack{k \geq 1 \\ j \geq 0}} \sum_{a_1, \dots, a_k} \frac{1}{k!} A_j(h) [\dots [a_1 D_{a_1 0}, D_{a_2 0}], \dots, D_{a_k 0}] \\ & - \sum_{\substack{k, m \geq 1 \\ a_1, \dots, a_k}} \frac{1}{k!} [\dots [\sigma c_1^+(m), D_{a_1 0}], \dots, D_{a_k 0}] \end{aligned}$$

$$\begin{aligned}
& - \sum_{k \geq 2} \frac{1}{k!} [\dots [V_0, \underbrace{D_{00}, \dots, D_{00}}_{k-1 \text{ times}}] \\
& - \sum_{k \geq 1} \frac{1}{k!} [\dots [\sigma c_1(0), \underbrace{D_{00}, \dots, D_{00}}_{k \text{ times}}]
\end{aligned}$$

In the first and second sums the indices a_i run over $\mathbb{Z}^0(p)$ with the restrictions $a_1 + \dots + a_k = c_0 + pj$ in the first case and $a_1 + \dots + a_k = pm$ in the second case.

Definition. For $n \geq 0$, denote by $\mathcal{F}_{\gamma, [n, 0]}^+$ the partial sum of $\mathcal{F}_{\gamma, [n, 0]}^0$ which contains only the terms with $[\dots [D_{a_1 \bar{n}_1}, D_{a_2 \bar{n}_2}], \dots, D_{a_s \bar{n}_s}]$ such that if for some $i_1 \geq 0$, $0 = n_s = \dots = n_{s-i_1} < n_{s-i_1-1}$ then at least one of a_s, \dots, a_{s-i_1} is not zero.

The following lemma follows directly from the above definition.

Lemma 5.2. *The sum of the first two lines in the RHS of (5.3) equals*

$$- \sum_{\substack{0 \leq n < N^* \\ j \geq 0}} \sigma^n(A_j(h)) \mathcal{F}_{c_0 + pj, [n, 0]}^+$$

Proof. For the first line use the above definition with $n = 0$.

For the second line use the following identity

$$\sum_{\substack{k \geq 1 \\ a_1, \dots, a_k}} (1/k!) [\dots [\sigma^{n+1} \mathcal{F}_{\gamma, -n}^0, D_{a_1 0}], \dots, D_{a_k}] = \mathcal{F}_{c_0 + pj, [n, 0]}^+$$

where $n \in \mathbb{N}$, $\gamma < c_0 + pj$ and a_1, \dots, a_k run over $\mathbb{Z}^0(p)$ such that $a_1 + \dots + a_k = p^{n+1}(c_0 + pj - \gamma)$. \square

Introduce the operators

$$G_0 = \widetilde{\exp}(\alpha_0 \text{ad} D_0), \quad F_0 = E_0(\alpha_0 \text{ad} D_0)$$

on \mathcal{L}_k (recall that $E_0(x) = (\widetilde{\exp} x - 1)/x$). Note that for $l \in \mathcal{L}_k$,

$$F_0(l) = \sum_{k \geq 1} \frac{\alpha_0^{k-1}}{k!} [\dots [l, \underbrace{D_0, \dots, D_0}_{k-1 \text{ times}}], \quad G_0(l) = \sum_{k \geq 0} \frac{\alpha_0^k}{k!} [\dots [l, \underbrace{D_0, \dots, D_0}_{k \text{ times}}].$$

With this notation we can rewrite (5.3) in the following form

$$(G_0 \sigma - \text{id})c_1(0) + F_0(V_0) = - \sum_{j \geq 0} \sum_{0 \leq i < N^*} \sigma^n(A_j(h)) \mathcal{F}_{c_0 + pj, [i, 0]}^+$$

Lemma 5.3. *Suppose $l(\alpha, \gamma) = \sum_{0 \leq i < N^*} \sigma^i(\alpha \mathcal{F}_{\gamma, -i}^0)$, where $\alpha \in k$. Then (recall $\tilde{N} = N^* - 1$, cf. Subsection 4.3)*

$$(G_0 \sigma - \text{id})l(\alpha, \gamma) = - \sum_{0 \leq i < N^*} \sigma^i(\alpha) \mathcal{F}_{\gamma, [i, 0]}^+ + \sigma^{N^*}(\alpha \mathcal{F}_{\gamma, -\tilde{N}}^0)$$

Proof of lemma. Directly from definitions it follows for $i \geq 0$, that $(G_0\sigma)(\sigma^i \mathcal{F}_{\gamma,-i}^0) = \sigma^{i+1} \mathcal{F}_{\gamma,-(i+1)}^0 - \mathcal{F}_{\gamma,[i+1,0]}^+$. Therefore,

$$\begin{aligned} (G_0\sigma)l(\alpha, \gamma) &= \sum_{1 \leq i \leq N^*} \sigma^i(\alpha \mathcal{F}_{\gamma,i}^0) - \sum_{1 \leq i \leq N^*} (\sigma^i \alpha) \mathcal{F}_{\gamma,[i,0]}^+ \\ &= l(\alpha, \gamma) - \sum_{0 \leq i < N^*} (\sigma^i \alpha) \mathcal{F}_{\gamma,[i,0]}^+ + \sigma^{N^*}(\alpha) \left(-\mathcal{F}_{\gamma,[N^*,0]}^+ + \sigma^{N^*} \mathcal{F}_{\gamma,-N^*} \right). \end{aligned}$$

It remains to note that $-\mathcal{F}_{\gamma,[N^*,0]}^+ + \sigma^{N^*} \mathcal{F}_{\gamma,-N^*} = \sigma^{N^*} \mathcal{F}_{\gamma,\tilde{N}}^0$. \square

Summarize the above calculations.

Proposition 5.4. *If $h_{<p}$ is a lift of h , $c_1 = c_1^- + c(0) + c_1^+$ and $V_0 = \alpha_0(\text{adh}_{<p})D_0$ then c_1^+ is given by Proposition 5.1 and*

$$c_1(0) = c^0 + \sum_{\substack{0 \leq i < N^* \\ j \geq 0}} \sigma^i(A_j(h) \mathcal{F}_{c_0+pj,-i}^0) \in \mathcal{L}_k,$$

where $c^0 \in \mathcal{L}_k$ and $V_0 \in \alpha_0 \mathcal{L}$ are solutions of the equation

$$(5.4) \quad (G_0\sigma - \text{id})c^0 + F_0(V_0) = \sigma^{N^*} \Omega^0,$$

$$\text{and } \Omega^0 = \sum_{j \geq 0} \left(A_j(h) \mathcal{F}_{c_0+pj,-\tilde{N}}^0 \right).$$

Remark. a) Modulo the ideal $[\mathcal{L}_k, D_0]$ of \mathcal{L}_k equation (5.4) admits explicit solution and, therefore, for any $h_{<p}$,

$$\text{adh}_{<p}(D_0) \equiv (\text{id}_{\mathcal{L}} \otimes \text{Tr}_{k/\mathbb{F}_p}) \Omega^0 \equiv \sum_{0 \leq n < N_0} \sigma^n(\Omega^0) \bmod [\mathcal{L}_k, D_0];$$

b) if $k = \mathbb{F}_p$ then $\sigma = \text{id}$ and there is $h_{<p}$ such that $\text{adh}_{<p}(D_0) = \Omega^0$; this is an explicit form of the Demushkin relation in L_h ;

c) it can be easily proved that (5.4) has solutions such that $c^0 \in \mathcal{L}_k^{(c_0)}$ and $V_0 \in \alpha_0 \mathcal{L}^{(c_0)}$ (use that $\Omega^0 \in \mathcal{L}_k^{(c_0)}$ and work modulo descending series of ideals $\text{ad}^s D_0(\mathcal{L}_k)$, $s \in \mathbb{N}$); then Theorem 4.4c) implies that the appropriate lift $h_{<p}$ is arithmetical;

d) the appearance of operators F_0 and G_0 in the LHS of (5.4) is related to a “bad influence” of the generators $D_{0\bar{n}}$ for $\bar{n} = n \bmod N_0 \in \mathbb{Z}/N_0$; this influence can be seen already at the explicit expressions of the elements $\mathcal{F}_{\gamma,-N}^0$ from Subsection 1.4: the elements of the form D_{0n} don’t contribute to γ and therefore can appear with almost no restrictions in all terms of $\mathcal{F}_{\gamma,-N}^0$, e.g. if $a \in \mathbb{Z}^0(p)$ then $\mathcal{F}_{a,-N}^0$ contains together with the linear term aD_{a0} all terms of the following expression $(\sigma^{-N}G_0)(\sigma^{-N+1}G_0) \dots (\sigma^{-1}G_0)F_0(aD_{a0})$.

6. APPLICATIONS TO THE MIXED CHARACTERISTIC CASE

Let K be a finite field extension of \mathbb{Q}_p with the residue field $k \simeq \mathbb{F}_{p^{N_0}}$ and the ramification index e_K . Let π_0 be a uniformising element in K . Denote by \bar{K} an algebraic closure of K and set $\Gamma_K = \text{Gal}(\bar{K}/K)$. Assume that K contains a primitive p -th root of unity ζ_1 .

6.1. For $n \in \mathbb{N}$, choose $\pi_n \in \bar{K}$ such that $\pi_n^p = \pi_{n-1}$. Let $\tilde{K} = \bigcup_{n \in \mathbb{N}} K(\pi_n)$, $\Gamma_{< p} := \Gamma_K / \Gamma_K^p C_p(\Gamma_K)$ and $\Gamma_{\tilde{K}} = \text{Gal}(\bar{K}/\tilde{K})$. Then a natural embedding $\Gamma_{\tilde{K}} \subset \Gamma_K$ induces a continuous group homomorphism $\iota : \Gamma_{\tilde{K}} \rightarrow \Gamma_{< p}$.

We have $\text{Gal}(K(\pi_1)/K) = \langle \tau_0 \rangle^{\mathbb{Z}/p}$, where $\tau_0(\pi_1) = \pi_1 \zeta_1$. Let $j : \Gamma_{< p} \rightarrow \text{Gal}(K(\pi_1)/K)$ be a natural epimorphism.

Proposition 6.1. *The following sequence*

$$\Gamma_{\tilde{K}} \xrightarrow{\iota} \Gamma_{< p} \xrightarrow{j} \langle \tau_0 \rangle^{\mathbb{Z}/p} \rightarrow 1$$

is exact.

Proof. For $n \in \mathbb{N}$, let $\zeta_n \in \bar{K}$ be such that $\zeta_n^p = \zeta_{n-1}$.

Consider $\tilde{K}' = \bigcup_n K(\pi_n, \zeta_n)$. Then \tilde{K}'/K is Galois with the Galois group $\Gamma_{\tilde{K}'/K} = \langle \sigma, \tau \rangle$. Here for any $n \in \mathbb{N}$ and some $s_0 \in \mathbb{Z}$, $\sigma \zeta_n = \zeta_n^{1+ps_0}$, $\sigma \pi_n = \pi_n$, $\tau(\zeta_n) = \zeta_n$, $\tau \pi_n = \pi_n \zeta_n$ and $\sigma^{-1} \tau \sigma = \tau^{(1+ps_0)^{-1}}$.

Therefore, $C_2(\Gamma_{\tilde{K}'/K}) \subset \langle \tau^p \rangle \subset \Gamma_{\tilde{K}'/K}^p = \langle \sigma^p, \tau^p \rangle$, $\Gamma_{\tilde{K}'/K}^p C_p(\Gamma_{\tilde{K}'/K}) = \langle \sigma^p, \tau^p \rangle$ and we have a natural exact sequence

$$\langle \sigma \rangle \rightarrow \Gamma_{\tilde{K}'/K} / \Gamma_{\tilde{K}'/K}^p C_p(\Gamma_{\tilde{K}'/K}) \rightarrow \langle \tau \rangle \bmod \langle \tau^p \rangle = \langle \tau_0 \rangle^{\mathbb{Z}/p} \rightarrow 1.$$

Note that $\Gamma_{\tilde{K}'}$ together with a lift $\hat{\sigma} \in \Gamma_{\tilde{K}}$ of σ generate $\Gamma_{\tilde{K}}$.

The above short exact sequence implies that $\text{Ker}(\Gamma_{< p} \rightarrow \langle \tau_0 \rangle^{\mathbb{Z}/p})$ is generated by $\hat{\sigma}$ and the image of $\Gamma_{\tilde{K}'}$. So, the kernel coincides with the image of $\Gamma_{\tilde{K}}$ in $\Gamma_K(1)$. \square

6.2. Let R be Fontaine's ring. We have a natural embedding $k \subset R$ and an element $t = (\pi_n \bmod p)_{n \geq 0} \in R$. If $\mathcal{K} = k((t))$ and $R_0 = \text{Frac } R$ then \mathcal{K} is a closed subfield of R_0 and the theory of the field-of-norms functor [31] identifies R_0 with the completion $\hat{\mathcal{K}}_{\text{sep}}$ of the separable closure \mathcal{K}_{sep} of \mathcal{K} in R_0 . This allows us to identify $\mathcal{G} = \text{Gal}(\mathcal{K}_{\text{sep}}/\mathcal{K})$ with $\Gamma_{\tilde{K}} \subset \Gamma_K$.

We shall apply the results of the above sections and use the appropriate notation for our field \mathcal{K} , e.g. $\mathcal{G}_{< p} = \text{Gal}(\mathcal{K}_{< p}/\mathcal{K})$, where $\mathcal{K}_{< p}$ is the subfield of \mathcal{K}_{sep} fixed by $\mathcal{G}^p C_p(\mathcal{G})$. Note that we have a natural continuous morphism of groups ι of $\mathcal{G}_{< p}$ to $\Gamma_{< p}$, the first group is infinite but the second is finite (use that its module of generators K^*/K^{*p} is finite). Therefore, we obtain the following property.

Proposition 6.2. *The sequence*

$$\mathcal{G}_{< p} \xrightarrow{\iota} \Gamma_{< p} \xrightarrow{j} \langle \tau_0 \rangle^{\mathbb{Z}/p} \rightarrow 1$$

is exact.

6.3. Let $\eta \in \text{Iso}^0(\mathcal{K}, R_0)$, cf. Subsection 4.1, and let $\eta_{<p} \in \text{Iso}^0(\mathcal{K}_{<p}, R_0)$ be a lift of η . Any such lift $\eta_{<p}$ can be specified by a choice of the image $(\text{id}_{\mathcal{L}} \otimes \eta_{<p})f \in \{f' \in \mathcal{L}_{R_0} \mid \sigma f' = (\text{id}_{\mathcal{L}} \otimes \eta)e \circ f'\}$. (The elements $e \in \mathcal{L}_{\mathcal{K}}$ and $f \in \mathcal{L}_{\mathcal{K}_{sep}}$ were chosen in Subsection 1.3.)

Let $c_0 := e_K p / (p-1)$. As earlier, consider $\mathcal{M} \subset \mathcal{L}_{\mathcal{K}}$, $\mathcal{M}_{<p} \subset \mathcal{L}_{\mathcal{K}_{sep}}$ and define similarly $\mathcal{M}_{R_0} \subset \mathcal{L}_{R_0}$, cf. Subsection 2.4. We know that $e \in \mathcal{M}$, $f \in \mathcal{M}_{<p}$ and for similar reasons, $(\text{id}_{\mathcal{K}} \otimes \eta_{<p})f \in \mathcal{M}_{R_0}$.

Proposition 6.3. *Suppose $(\text{id}_{\mathcal{L}} \otimes \eta)e \equiv e \pmod{t^{(p-1)c_0} \mathcal{M}_{R_0}}$. Then*

a) *there is $c \in t^{(p-1)c_0} \mathcal{M}_{R_0}$ such that $(\text{id}_{\mathcal{L}} \otimes \eta)e = (-\sigma c) \circ e \circ c$;*

b) *for any lift $\eta_{<p}$ of η , there is a unique $l \in G(\mathcal{L}/\mathcal{L}(p))$ such that*

$$(\text{id}_{\mathcal{L}} \otimes \eta_{<p})f \equiv f \circ l \pmod{t^{(p-1)c_0} \mathcal{M}_{R_0}};$$

Proof. a) Note that $t^{(p-1)c_0} \mathcal{M}_{R_0}$ is an ideal in \mathcal{M}_{R_0} and for any $i \in \mathbb{N}$ and $m \in t^{(p-1)c_0} C_i(\mathcal{M}_{R_0})$, we can always find $c_i \in t^{(p-1)c_0} C_{i+1}(\mathcal{M}_{R_0})$ such that $\sigma c_i - c_i = m$.

Therefore, there is $c_1 \in t^{(p-1)c_0} \mathcal{M}_{R_0}$ such that $\eta(e) = e - \sigma c_1 + c_1$. This implies that $\sigma(c_1) \circ \eta(e) \equiv e \circ c_1 \pmod{t^{(p-1)c_0} C_2(\mathcal{M}_{R_0})}$. Similarly, there is $c_2 \in t^{(p-1)c_0} C_2(\mathcal{M}_{R_0})$ such that $\sigma(c_1) \circ \eta(e) = -\sigma c_2 + c_2 + e \circ c_1$ and $\sigma(c_2 \circ c_1) \circ \eta(e) \equiv e \circ (c_2 \circ c_1) \pmod{t^{(p-1)c_0} C_3(\mathcal{M}_{R_0})}$ and so on.

After $p-1$ iterations we obtain $c_i \in t^{(p-1)c_0} C_i(\mathcal{M}_{R_0})$, $1 \leq i < p$, such that $\sigma(c_{p-1} \circ \dots \circ c_1) \circ \eta(e) = e \circ (c_{p-1} \circ \dots \circ c_1)$. This proves a).

b) Let $(\text{id}_{\mathcal{L}} \otimes \eta_{<p})f = f'$. Then $\sigma(c \circ f') = e \circ (c \circ f')$. Therefore, there is $l \in \mathcal{L}$ such that $c \circ f' = f \circ l$. This proves the existence of l . Such l is unique modulo $\mathcal{L}(p)$ because $t^{c_0(p-1)} \mathcal{M}_{R_0} \subset \mathcal{L}_{m_R} + \mathcal{L}(p)_{R_0}$. \square

6.4. Let $\varepsilon = (\zeta_n \bmod p)_{n \geq 0} \in R$ be Fontaine's element (here $\zeta_0 = 1$ and the others ζ_n were introduced in Subsection 6.1).

Let $\zeta_1 = 1 + \sum_{i \geq 1} [\beta_i] \pi_0^i$ where $[\beta_i]$ are Teichmüller representatives of $\beta_i \in k$. Use the rings identification $R/t^{pe_K} \simeq O_{\bar{K}}/p$, coming from the natural projection $R \rightarrow (O_{\bar{K}}/p)_1$. This implies that

$$\varepsilon \equiv 1 + \sum_{i \geq 0} \alpha_i t^{c_0 + pi} \pmod{t^{pc_0}}$$

where all $\alpha_i \in k$, $\alpha_0 = 0$.

Assume that the morphism $h \in \text{Aut} \mathcal{K}$ from Subsection 2.1 is such that for all i , $\alpha_i(h) = \alpha_i$.

Clearly, $h(t) \equiv \tau_0(t) \pmod{t^{c_0(p-1)} \mathcal{M}_{R_0}}$, hence $\eta := \tau_0 \cdot h^{-1} \in \text{Iso}^0(\mathcal{K}, R_0)$ satisfies the assumption from Proposition 6.3b). This easily implies that the orbits of $f \pmod{t^{(p-1)c_0} \mathcal{M}_{R_0}}$ with respect to the action of Γ_K and $\tilde{\mathcal{G}}_h$ coincide. Therefore, there is a surjective map of sets $\kappa : \Gamma_K \rightarrow \mathcal{G}_h$.

Proposition 6.4. *κ induces a group isomorphism $\kappa(1) : \Gamma_{<p} \rightarrow \mathcal{G}_h$.*

Proof. Recall that we have the field-of-norms identification $\Gamma_{\tilde{K}} = \mathcal{G}$ and, therefore, κ identifies the groups $\kappa(\Gamma_{\tilde{K}}) = G(\mathcal{L}/\mathcal{L}(p))$. Choose a lift τ of τ_0 to Γ_K such that

$$(\text{id}_{\mathcal{L}} \otimes \tau)f \equiv (\text{id}_{\mathcal{L}} \otimes h_{<p})f \bmod t^{c_0(p-1)}\mathcal{M}_{R_0}.$$

Prove that κ is group homomorphism by verifying the following two properties (we use the abbreviation $A = \text{Ad } h_{<p}$ and the identification $\eta_0 : \mathcal{G}_{<p} \rightarrow G(\mathcal{L})$ from Subsection 1.3):

a) for any $m \in \mathbb{N}$, $\kappa(\tau^m) = h_{<p}^m$;

b) for any $l \in \mathcal{L} \bmod \mathcal{L}(p)$, $\eta_0(\text{Ad } \kappa(\tau)(\eta_0^{-1}l)) \equiv A(l) \bmod \mathcal{L}(p)$.

Let $(\text{id}_{\mathcal{L}} \otimes h_{<p})f \equiv c \circ (A \otimes \text{id}_{\mathcal{K}_{<p}}) \bmod t^{c_0(p-1)}\mathcal{M}_{R_0}$.

Then by induction on $m \geq 0$ we obtain the following congruences modulo $t^{c_0(p-1)}\mathcal{M}_{R_0}$

$$\begin{aligned} \kappa(\tau^{m+1}) &\equiv \kappa(\tau^m)\kappa(\tau)f \equiv \kappa(\tau^m)(c \circ (A \otimes \text{id}_{\mathcal{K}_{<p}}))f \equiv \\ &(\text{id}_{\mathcal{L}} \otimes h_{<p}^m)c \circ (A \otimes \kappa(\tau^m))f \equiv (\text{id}_{\mathcal{L}} \otimes h_{<p}^m)c \circ (A \otimes h_{<p}^m)f \\ &\equiv (\text{id}_{\mathcal{L}} \otimes h_{<p}^m)(c \circ (A \otimes \text{id}_{\mathcal{K}_{<p}}))f \equiv (\text{id}_{\mathcal{L}} \otimes h_{<p}^{m+1})f \end{aligned}$$

(use that $(\text{id}_{\mathcal{L}} \otimes h)c \equiv (\text{id}_{\mathcal{L}} \otimes \kappa(\tau_0))c$ and that $A \otimes \text{id}_{\mathcal{K}_{<p}}$ commutes with $\text{id}_{\mathcal{L}} \otimes h_{<p}$ and $\text{id}_{\mathcal{L}} \otimes \kappa(\tau)$.) This proves a). Similarly,

$$\begin{aligned} (\text{id}_{\mathcal{L}} \otimes \kappa(\tau^{-1}\eta_0(l)\tau))f &\equiv (\text{id}_{\mathcal{L}} \otimes \kappa(\tau^{-1}\eta_0(l)))(c \circ (A \otimes \text{id}_{\mathcal{K}_{<p}}))f \\ &\equiv (\text{id}_{\mathcal{L}} \otimes \kappa(\tau)^{-1})(c \circ (A \otimes \text{id}_{\mathcal{K}_{<p}}))(f \circ l) \equiv f \circ A(l) \end{aligned}$$

and b) is proved.

Prove that $\kappa(1)$ is isomorphism.

The number of minimal generators of $\Gamma_{<p}$ equals $\text{rk}_{\mathbb{F}_p}(K^*/K^{*p}) = [K : \mathbb{Q}_p] + 2 = e_K N_0 + 2$. If \mathfrak{G} is a free pro- p -group with $e_K N_0 + 2$ generators then we have a group epimorphism $j_K : \mathfrak{G}_{<p} \rightarrow \Gamma_{<p}$. We also know that Γ_K has one (Demushkin) relation of a very special form [27]. Therefore $\text{Ker } j_K$ is a normal subgroup in $\mathfrak{G}_{<p}$ generated as a normal subgroup by one element from $C_2(\mathfrak{G}_{<p}) \setminus C_3(\mathfrak{G}_{<p})$. This can be translated to the language of Lie \mathbb{F}_p -algebras: if $\mathfrak{G}_{<p} = G(\mathfrak{L})$, $\Gamma_{<p} = G(L)$ then $j_K : \mathfrak{L} \rightarrow L$ is epimorphism of Lie algebras and $\text{Ker } j_K$ is an ideal $\langle l_K \rangle$ of \mathfrak{L} generated by some $l_K \in C_2(\mathfrak{L}) \setminus C_3(\mathfrak{L})$.

According to Subsection 3.6 $L_{h,k}$ has a minimal system of k -generators

$$\{D_{an} \mid a \in \mathbb{Z}^+(p) \cap [1, c_0], n \in \mathbb{Z}/N_0\} \cup \{D_0\} \cup \{h_{<p}\}.$$

This set has $c_0(1 - 1/p)N_0 + 2 = e_K N_0 + 2$ elements (recall that $c_0 = e_K p/(p-1)$) and, therefore, we have epimorphism of Lie algebras $j_h : \mathfrak{L} \rightarrow L_h$. There is also only one relation $l_h \in C_2(\mathfrak{L}) \setminus C_3(\mathfrak{L})$.

Finally, we can assume that $\kappa(1)$ is induced by the identity morphism of \mathfrak{L} and, therefore, we have embedding of ideals $\langle l_K \rangle \subset \langle l_h \rangle$. It remains to prove the following lemma.

Lemma 6.5. l_K generates the ideal $\langle l_h \rangle$.

Proof of lemma. Let $\mathcal{I} = \langle l_h \rangle$. For $s \geq 0$, let $\mathcal{I}(s)$ be a submodule in \mathfrak{L} generated by the elements of the form $[\dots [l_h, l_1], \dots, l_{s_1}]$, where all $l_i \in \mathfrak{L}$ and $s_1 \geq s$. Clearly, $\mathcal{I}(s)$ is a decreasing sequence of ideals in \mathfrak{L} , $\mathcal{I}(0) = \mathcal{I}$ and $\mathcal{I}(p-2) = 0$.

Now note that $l_K \bmod C_3(\mathfrak{L})$ is non-zero and, therefore, we can assume that $l_K \equiv l_h \bmod C_3(\mathfrak{L})$. Then for all s , $\mathcal{I}(s) \subset \langle l_K \rangle + \mathcal{I}(s+1)$. (Just use the definition of $\mathcal{I}(s)$.) Iterating this relation we obtain that $\mathcal{I} = \mathcal{I}(0) \subset \langle l_K \rangle + \mathcal{I}(p-1) = \langle l_K \rangle$. The lemma is proved. \square

\square

Recall that $\Gamma_{<p}$ has the induced filtration by the ramification subgroups $\Gamma_{<p}^{(v)}$, where $v \geq 0$. This gives the appropriate filtration by ideals $L^{(v)}$ of the Lie algebra L . Note that all elements of Γ_K appear as continuous automorphisms of $R_0 = \mathcal{K}_{sep}$, where \mathcal{K} is the field-of-norms of the extension \tilde{K}/K and, therefore, can be considered as elements of ramification subsets $\mathcal{I}_{\mathcal{K}}^{(v)}$, $v \geq 0$, cf. Subsection 4.1. This gives the induced filtration $L_{/\mathcal{K}}^{(v)}$ on L . Using the property of compatibility of the field-of-norms functor with ramification filtrations we obtain that

$$L_{/\mathcal{K}}^{(v_K)} = L^{(v_K)}$$

where $v_K = \varphi_{\tilde{K}/K}(v_{\mathcal{K}})$ and $\varphi_{\tilde{K}/K}$ is the Herbrand function for the extension \tilde{K}/K .

On the other hand, the elements of $\mathcal{G}_h = G(L_h)$ come also from $\mathcal{I}_{\mathcal{K}}$ and we have the induced ramification filtration by ideals $L_h^{(v)}$, $v \geq 0$.

Proposition 6.6. *For any $v \geq 0$, $\kappa(1)(L_{/\mathcal{K}}^{(v)}) = L_h^{(v)}$.*

Proof. Let $\tilde{\Gamma} = G(\tilde{L})$ be the image of $\Gamma_{\tilde{K}}$ in $\Gamma_{<p}$. Then $\kappa(1)(\tilde{\Gamma}) = G(\mathcal{L}/\mathcal{L}(p))$ and this identification comes from identification $\Gamma_{\mathcal{K}} = \mathcal{G}$ given by the field-of-norms functor. Therefore, for any $v \geq 0$,

$$(6.1) \quad \kappa(1)(L_{/\mathcal{K}}^{(v)} \cap \tilde{L}) = L_h^{(v)} \cap (\mathcal{L}/\mathcal{L}(p)).$$

Suppose $h_{<p}$ is an arithmetical lift of h then $h_{<p} \in L_h^{(c_0)}$ and for any $v > c_0$, $h_{<p} \notin L_h^{(v)}$. Similarly, if $\tau_{<p}$ is an arithmetical lift of τ_0 then $\tau_{<p} \in L_{/\mathcal{K}}^{(c_0)}$ and for any $v > c_0$, $h_{<p} \notin L_{/\mathcal{K}}^{(v)}$. Therefore, (6.1) proves our proposition for all $v > c_0$. The case $v \leq c_0$ will be implied by the following lemma.

Lemma 6.7. *$\tau_{<p}$ is arithmetical iff $h_{<p} = \kappa(1)(\tau_{<p})$ is arithmetical.*

Proof of lemma. Suppose $\tau_{<p}$ is arithmetical. Then similarly to Subsection 4.2 we have

$$(\text{id}_{\mathcal{L}} \otimes \tau_{<p})f \equiv c \circ f \bmod \mathcal{L}_{R_0}^{(c_0)}.$$

Then we can proceed word-by-word similarly to Subsections 4.4 -4.5 with $h_{<p}$ replaced by $\tau_{<p}$ to obtain that c satisfies the condition from

Theorem 4.4b). But $(\text{id}_{\mathcal{L}} \otimes h_{<p})f$, where $h_{<p} = \kappa(1)\tau_{<p}$ has the same c and, therefore, $h_{<p}$ is also arithmetical. Obviously, this also proves the “only if” part of our lemma. \square

\square

6.5. The list of properties of $\Gamma_{<p} = G(L)$. As a result we have the following construction of the Galois group $\Gamma_{<p}$ together with its ramification filtration $\{\Gamma_{<p}^{(v)}\}_{v \geq 0}$.

- *Group structure:*

- $\Gamma_{<p} = G(L)$, where L is the Lie \mathbb{F}_p -algebra such that

$$0 \longrightarrow \mathcal{L}/\mathcal{L}(p) \longrightarrow L \longrightarrow \mathbb{F}_p\tau_0 \longrightarrow 0.$$

- the Lie algebra \mathcal{L} was defined in Subsection 1.3;

- \mathcal{L}_k has standard system of generators

$$\{D_{an} \mid a \in \mathbb{Z}^+(p), n \in \mathbb{Z}/N_0\} \cup \{D_0\}$$

- the ideals $\mathcal{L}(s)$, $2 \leq s \leq p$, are given by Theorem 2.3 and $C_s(L) = \mathcal{L}(s)/\mathcal{L}(p)$;

- the structure of L is determined by a lift $\tau_{<p}$ of τ_0 and the appropriate differentiation $\text{ad}\tau_{<p}$ described via recurrent relation (3.4), cf. also more explicit information from Section 5.

- *The ramification filtration:*

- if $K_{\leq s} := K_{<p}^{C_{s+1}(L)}$ then the maximal upper ramification number for $K_{\leq s}/K$ is $c_0 = e_K p/(p-1)$ if $s = 1$ and $c_0 + (c_0(s-1) - 1)/p = e_K(1 + s/(p-1)) - 1/p$ if $2 \leq s < p$ (use the estimate from Subsection 2.5 and the Herbrand function $\varphi_{K(\pi_1)/K}$);

- $\tau_{<p}$ is arithmetical, i.e. $\tau_{<p} \in L^{(c_0)}$, iff the appropriate solutions c_1 and $\{V_a \mid a \in \mathbb{Z}^0(p)\}$ of (3.4) satisfy the criterion from Theorem 4.4;

- if $v \leq c_0$ and $\tau_{<p}$ is arithmetical then $\Gamma_{<p}^{(v)}$ is the subgroup of $\Gamma_{<p}$ generated by the image of $G(\mathcal{L}^{(v)})$ and $\tau_{<p}$ (the ideals $\mathcal{L}^{(v)}$ are described in Subsection 1.4);

- if $v > c_0$ then $\Gamma_{<p}^{(v)}$ is the image of $G(\mathcal{L}^{(v^*)})$, where $v^* = c_0 + p(v - c_0)$ (use the Herbrand function for $K(\pi_1)/K$);

- for explicit information about Demushkin relation for L , i.e. about the element $\text{ad}\tau_{<p}(D_0)$, cf. the end of Subsection 5.2.

REFERENCES

- [1] V.A.ABRASHKIN, *Ramification filtration of the Galois group of a local field*, Proceedings of the St. Petersburg Mathematical Society III, Amer. Math. Soc. Transl. Ser. 2, (1995) **166**, Amer. Math. Soc., Providence, RI
- [2] V.A. ABRASHKIN, *Ramification filtration of the Galois group of a local field. II*, Proceedings of Steklov Math. Inst. **208** (1995)
- [3] V.ABRASHKIN, *Ramification filtration of the Galois group of a local field. III*, Izvestiya RAN: Ser. Mat., **62**, no.5 (1998), 3-48; English transl. Izvestiya: Mathematics **62**, no.5, 857–900
- [4] V.A. ABRASHKIN *A group-theoretical property of the ramification filtration*, Izvestiya RAN: Ser. Mat., **62**, no.6 (1998), 3-26; English transl. Izvestiya: Mathematics **62**, no.6 (1998), 1073–1094
- [5] V.ABRASHKIN, *Report on the ramification filtration of the Galois group of a local field*, Proceedings of the Research Conference on “Number Theory and Arithmetical Geometry: Arithmetical applications of Modular Forms” (San Feliu de Guixols, Spain, 24-29 October, 1997) Inst. fur Exp. Math. Universitat Essen, 1998, 47-53
- [6] V. ABRASHKIN, *On a local analogue of the Grothendieck Conjecture*, Int. J. Math. (2000) **11**, no.1, 3–43
- [7] V. ABRASHKIN, *Ramification theory for higher dimensional fields*, Contemp. Math. (2002) **300**, 1-16
- [8] V. ABRASHKIN, *Characteristic p case of the Grothendieck conjecture for 2-dimensional local fields*, Proceedings of Steklov Institute (2003) **241**, 1-35
- [9] V. ABRASHKIN, *Characteristic p analogue of modules with finite crystalline height*, Pure Appl. Math. Q., **5** (2009), 469–494
- [10] V. ABRASHKIN, *Modified proof of a local analogue of the Grothendieck Conjecture*. Journal Théorie des Nombres de Bordeaux **22**, (2010), 1-50
- [11] V.ABRASHKIN, *Galois groups of local fields, Lie algebras and ramification*, 2014, 21 pages
- [12] V.ABRASHKIN, R.JENNI *The field-of-norms functor and the Hilbert symbol for higher local fields* J.Théor. Nombres Bordeaux, **24** (2012), no.1, 1-39
- [13] A.BONFIGLIOLI, R.FULCI, *Topics in Noncommutative Algebra*, Lecture Notes in Mathematics 2034, Springer-Verlag Berlin heidelberg 2012
- [14] N. BOURBAKI, *Elements of Mathematics. Lie Groups and Lie Algebras*.
- [15] P.DELIGNE *Les corps locaux de caractéristique p , limites de corps locaux de caractéristique 0*, Representations of reductive groups over a local field, Travaux en cours, Hermann, Paris, 1973, 119-157
- [16] N.L.GORDEEV, *Ramification groups of infinite p -extensions of a local field*, Soviet Math. **20**, no.6 (1982)
- [17] N.L.GORDEEV, *Infinity of the number of relations in the Galois group of the maximal p -extension of a local field with bounded ramification*, Izvestia AN SSSR, Ser. Matem. (1981) **45**, 592-607
- [18] M. HALL *The theory of groups*, The Macmillan Company New York, 1959
- [19] U.JANNSEN, K.WINGBERG, *Die Struktur der absoluten Galoisgruppe p -adischer Zahlkörper*, Invent. math. (1982) **70**, 71-98
- [20] H.KOCH, *Galois theory of p -extensions*, Springer Monographs in Mathematics, 2002, XIII, 191 p
- [21] H.KOCH, E. DE SHALIT, *Metabelian local class field theory* J. Reine Angew. Math. (1996) **478**, 85-106
- [22] F. LAUBIE *Extensions de Lie et groupes d'automorphismes de corps locaux*, Comp. Math., **67** (1988), 165-189

- [23] F.LAUBIE *Une théorie du corps de classes local non abélien* Compos. Math., **143** (2007), no. 2, 339362.
- [24] M. LAZARD, *Sur les groupes nilpotentes et les anneaux de Lie*, Ann. Ecole Norm. Sup. (1954) **71**, 101-190
- [25] SH.MOCHIZUKI, *A version of the Grothendieck conjecture for p -adic local fields*, Int. J. Math., **8**, no.4 (1997), 499-506
- [26] J.-P.SERRE, *Local Fields* Berlin, New York: Springer-Verlag, 1980
- [27] J.-P.SERRE, *Cohomologie Galoisienne* Springer Verlag, Berlin-Göttingen-Heidelberg-New York, 1964
- [28] J.-P.SERRE Bourbaki *Structure de certains pro- p -groupes (d'après Demukin)* Séminaire Bourbaki, **8**, Exp. No. 252, 145155, Soc. Math. France, Paris, 1995.
- [29] I.R. SHAFAREVICH, *On p -extensions (In Russian)*, Mat. Sbornik (1947) **20**, 351-363
- [30] J.-P. WINTENBERGER, *Le corps des normes de certaines extensions infinies des corps locaux; application* Ann. Sci. Ec. Norm. Super., IV. Ser, **16** (1983), 59-89
- [31] J.-P.WINTENBERGER, *Extensions de Lie et groupes d'automorphismes des corps locaux de caractéristique p* . (French) C. R. Acad. Sci. Paris Sér. **A-B** **288** (1979), no. 9, A477-A479
- [32] W. ZINK *Ramification in local Galois groups; the second central step*, Pure Appl. Math. Q. **5** (2009), no. 1, 295338.

DEPARTMENT OF MATHEMATICAL SCIENCES, DURHAM UNIVERSITY, SCIENCE
LABORATORIES, SOUTH RD, DURHAM DH1 3LE, UNITED KINGDOM & STEKLOV
INSTITUTE, GUBKINA STR. 8, 119991, MOSCOW, RUSSIA
E-mail address: victor.abrashkin@durham.ac.uk